User Manual:

ALB / ALB-X /ALB-VA

jetNEXUS Solutions Limited
Grove Business Park
Cedar Court
Waltham Road
Maidenhead
Berkshire
Sl6 3LW

Phone: 0870 382 5050 or International +44 (0) 1628 820 630
Fax: 0870 382 55 20 or International +44 (0) 1628 820 647

Author: jetNEXUS Solutions Limited
Reviewed: Greg Howett
Modified: Gary Christie
Version: 2.4 (2.1 Current) (1428)
Created: 08/09/2011
Release Date: 28/02/2012

Limitations: This document and all of its contents are provided as-is. jetNEXUS has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, jetNEXUS will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that jetNEXUS cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.

Table of Contents

5) jetNEXUS Connectivity Modes
    a. Managed
    b. Direct Server Return
    c. Transparency
    d. Gateway

Configuring a Channel Service

1) Adding a Load Balanced Service
2) Setup Channel Details
    a. Channel Descriptions
    b. Configuring a new Channel
3) Setup Destination Details
    a. Content Server Descriptions
    b. Configuring a new Content Server
    c. Adding additional Content servers
4) Setup Actions
    a. Actions Descriptions
5) Adding another service to the same channel
6) Adding an additional Channel IP
7) Channel Status lights

Server Health Monitoring

1) Server Health monitoring
2) Configuring server health Monitoring

flightPATH

1) What is flightPATH
2) What can flightPATH do
3) How can I access flightPATH
4) How do I build a flightPATH rule?
    a. Conditions
    b. Sense
    c. Check
    d. Evaluation
    e. Actions
5) How Do I apply flightPATH rules?

Caching

1) How jetNEXUS caching works
2) Parameters to configure overall cache behaviour
3) Parameters to define rule bases for Domains
4) Parameters to define on or more caching rule bases
5) Cache Settings
    a. Maximum cache size
    b. Desired cache size
    c. Default Caching time
    d. Cacheable HTTP response code
    e. Cache-fill count
6) Adding a Caching rule
7) Creating a caching rule base
8) Associating Domains to a caching rule base
    a. Caching by HOST
    b. Caching by Channel
9) Cache content Statistics

Connection Pooling

1) What is connection pooling?
2) Enable connection pooling.

SSL Offload and Termination

1) What can jetNEXUS can do with SSL
2) Creating a self-signed certificate
    a. Certificate name
    b. Organization
    c. Organizational unit
    d. City/Locality
    e. Sate/Province
    f. Country
    g. Domain name
    h. Key Length
    i. Period
3) Creating Certificate Requests
4) Installing trusted certificates
5) Certificate Management
    a. Renew

   b. Show
   c. Delete
   d. Install
6) Importing Certificates
7) Exporting Certificates
8) Configuring an SSL Listening interface
9) Configuring SSL for content servers

Failover Configuration

1) Why use failover?
2) Enabling failover
3) Failover diagram
4) Failover diagram explained
5) Failover configuration
6) Failover status lights

ALB Maintenance

1) Backing up the ALB
2) Restoring the ALB
3) Updating the software
4) Configuring logging
5) Passwords and security

Acceleration and Compression (Advanced)

1) Initial Thread memory Allocation
2) Maximum Thread memory
3) Increment Memory
4) Minimum compression size
5) Safe mode
6) Disable compression
7) Compress as you go
   a. By page request
   b. ON
   c. OFF
8) Compression exclusions

Monitoring

1) Dashboard
    a. Disk space
    b. Memory indication bar
    c. CPU indication bar
2) Events
3) Statistics
    a. Default statistics screen
    b. From Cache
    c. From Server
    d. Cache contents
    e. The CPU Usage
    f. The memory usage
    g. Overall hits counted

Logging

1) Download W3C Log
2) Download system log

E-mail Events

1) What can you set
2) Mail server (SMTP) setup
3) Services
    a. Data and time
    b. Ping
    c. SNMP
    d. Capture
    e. Restart
    f. Reboot
    g. Power off
4) Date and time
    a. Time server URL
    b. Update time
    c. Update Period
    d. NTP Method
5) Ping
6) SNMP

   a. SNMP v1/v2
   b. SNMP v3
   c. jetNEXUS ALB SNMP
7) Capture
8) Restart
9) Reboot
10) Power off
11) CLI (Command Line Interface)

jetNEXUS Help

1) FAQ's
2) Troubleshooting
3) Contact Us

jetNEXUS Introduction

Scope

The aim of this document is to provide a user manual and deployment overview for the jetNEXUS Accelerating Load balancer (ALB), Accelerating Load balancer Extreme (ALB-X), Accelerating Load balancer Virtual Appliance (ALB-VA) and Accelerating Load balancer Extreme Virtual Appliance(ALB-X VA), Products.

If you have any questions about this guide or require any assistance during your setup please do not hesitate to contact support@jetnexus.com or call us on 0870 382 5529 where one of our dedicated support team will be able to help with any questions or queries you have.

What is the jetNEXUS ALB?

The jetNEXUS Accelerating Load balancer (ALB) is an advanced load balancing and traffic management solution that enables clients to create and deliver fast, resilient, and scalable online services.

The ALB, ALB-X & ALB-VA are all Application Delivery Controllers (ADC) sometimes referred to as a next generation load balancer. The ALB-X is feature rich, delivering the advanced functionality you would expect from a market leading solution at a cost effective price point. Focusing on the features that make the biggest difference to end user experience, the ALB-X combines **Layer 7 Load Balancing**, **Compression**, **SSL Offload, SSL Re-encryption** and **Content Caching** in one comprehensive solution.

Features such as **dynamic data compression, SSL offload, connection management** and **content caching** work to reduce server load and optimize application contents for superb performance.

The ALB-X is a plug and play solution, available in a variety of formats. The GUI is intuitive with drag and drop functionality and SOAP API for easy management.

The ALB-X also features **flightPATH**, a powerful, scriptable Layer7 routing engine for the creation of traffic rules and intelligent service management.

How does Load Balancing Work?

The basic principle is that network traffic is sent to a shared IP, jetNEXUS call this the Channel IP. In some cased you may know this as a Virtual IP (VIP) or listening IP. This Channel IP is an address that it attached to the jetNEXUS. Once the jetNEXUS receives a request on this Channel IP it will need to make a decision on where to send it. This decision is normally controlled by a "load balancing method/ strategy", a "Server health check" or, in the case of a next generation device, a rule set.

The request is then sent to the appropriate server and the server will produce a response. Depending on the type of Load Balancing method selected, the response will be sent either back to the load balancer, in the case of Layer 7. With a layer 4 service it is sent directly back to the end user (normally via its default gateway)The jetNEXUS also acts as a proxy based load balancer; the request from the web server can be returned to the load balancer and manipulated before being sent back to the user. This manipulation can involve content substitution, or compression.

What are Load Balancing Methods / Strategies?

Typically a load balancing method or strategy is used to decide how the load balancer chooses where to send the request. Below are the methods used by jetNEXUS ALB.

Least Connections: The load balancer will keep track of the number of connections a back end server has and send the next request to the server with the least connections.

Round Robin: The simplest method, each back end server takes a turn.

IP Based: In this situation the clients IP address is used to select which back end server will receive the request. IP session persistence runs at layer 4 as such it can be used when load balancing non HTTP protocols. This method is useful for internal networks where the network topology is known and you can be confident that there are no "super proxies" upstream. If this is the case the all the requests will look like they are coming from one client, and as such the load would be uneven.

Cookie Based: This is the most popular persistence method for HTTP. In this situation, least connections load balancing is used for each first request. A cookie is inserted into the headers of the first http response. Thereafter, jetNEXUS ALB uses the client cookie to route traffic to the same back end server. Again this is used when the client must go to the same back end server each time.

Classic ASP Session Cookie: Active Server Pages (ASP) is a Microsoft server-side technology. With this option selected the ALB will maintain session persistence to the same server if an ASP cookie is detected and is found in its list of known cookies. If a new ASP cookie is detected then it will be load balanced using the least connections algorithm.

ASP.NET Session Cookie: ASP.NET is a Microsoft server-side technology. With this option selected the ALB will maintain session persistence to the same server if an ASP.NET cookie is detected and is found in its list of known cookies. If a new ASP.NET cookie is detected then it will be load balanced using the least connections algorithm.

JSP Session Cookie: Java Server Pages (JSP) is an Oracle server-side technology. With this option selected the ALB will maintain session persistence to the same server if a JSP cookie is detected and is found in its list of known cookies. If a new JSP cookie is detected then it will be load balanced using the least connections algorithm.

JAX-WS Session Cookie: Java web services (JAX-WS) is an Oracle server-side technology. With this option selected the ALB will maintain session persistence to the same server if a JAX-WS cookie is detected and is found in its list of known cookies. If a new JAX-WS cookie is detected then it will be load balanced using the least connections algorithm.

PHP Session Cookie: Personal Home Page (PHP) is an open source server-side technology. With this option selected the ALB will maintain session persistence to the same server if a PHP cookie is detected.

What is an Application Delivery Controller (ADC)

ADC's are designed for applications and improve the performance of Web-based and related applications by providing a suite of services at the network and application layers. Advanced ADC's become actively involved in the delivery of the application and provides sophisticated capabilities, as opposed to Server load balancing solutions that typically perform a basic set of functions, including load balancing, basic health checks and Secure Sockets Layer (SSL) offload processing.

Advanced platform ADCs provide the basic Server Load Balancing functionality and additionally provide support for real-time protocol manipulation (for example, Transmission Control Protocol [TCP] connection management and HTML optimization), data compression, network address translation, quality of service (QOS), DOS protection, SSL Offload and resiliency/failover. These devices are being enhanced by the addition of new protocol intelligence and new services, such as content transformation and transaction assurance.

jetNEXUS Benefits

The ALB-X negates the costly effects of data center server sprawl, dramatically improving the performance and efficiency of web servers to ensure high application availability and service quality. The ALB-X represents the next generation in web load balancing by delivering advanced ADC features in a comprehensive yet cost effective solution that is flexible to deploy and easy to manage.

High Availability for your Mission Critical Business Applications

The ALB is an essential network component, key to guaranteeing server availability and delivering a reliable online service. The ALB can be deployed in a high availability pair to enable fail over and remove any single point of failure.

The ALB-X **server health monitoring** feature can detect and route around problem servers to eliminate downtime. **Advanced reporting** and **logging** provides real time performance and availability stats for comprehensive monitoring and analysis.

Features such as **dynamic data compression**, **SSL offload**, **connection management** and **content caching** work to reduce server load and optimize application contents for superb performance.

The ALB-X also features **flightPATH**, a powerful, scriptable Layer7 routing engine for the creation of traffic rules and intelligent service management.

jetNEXUS ALB

- *Guarantee Service Delivery*
- *Accelerate Applications*
- *Non Stop Application Availability*
- *Increase Network Resiliency*
- *Implement Traffic Routing Rules*
- *Improve End-User Experience*
- *Reduce Bandwidth Consumption*
- *For Reliable, Scalable Services*

jetNEXUS Configuration

Basic Configuration and First boot

On first boot jetNEXUS will boot and try to obtain an IP address via DHCP. If there is no DHCP server present it will boot with its default IP of **192.168.100.100** on subsequent boots the DHCP client then disabled.

The simplest way to initially configure the ALB-X is to use the jetNEXUS Discovery windows application.

The jetNEXUS discovery application will scan the local network looking for ALB's and allow you to perform some basic configuration such as set a management IP/ default gateway etc.

If you are implementing into a subnet where there is no DHCP and you are not be able to contact it using jetNEXUS discovery, due to network restrictions or the fact that the network is secure/private you can access the web GUI on https://192.168.100.100:27376 this may require some configuration changes on the machine you are using to configure the appliance i.e. adding a new IP address on machine into the same subnet as 192.168.100.100/24.

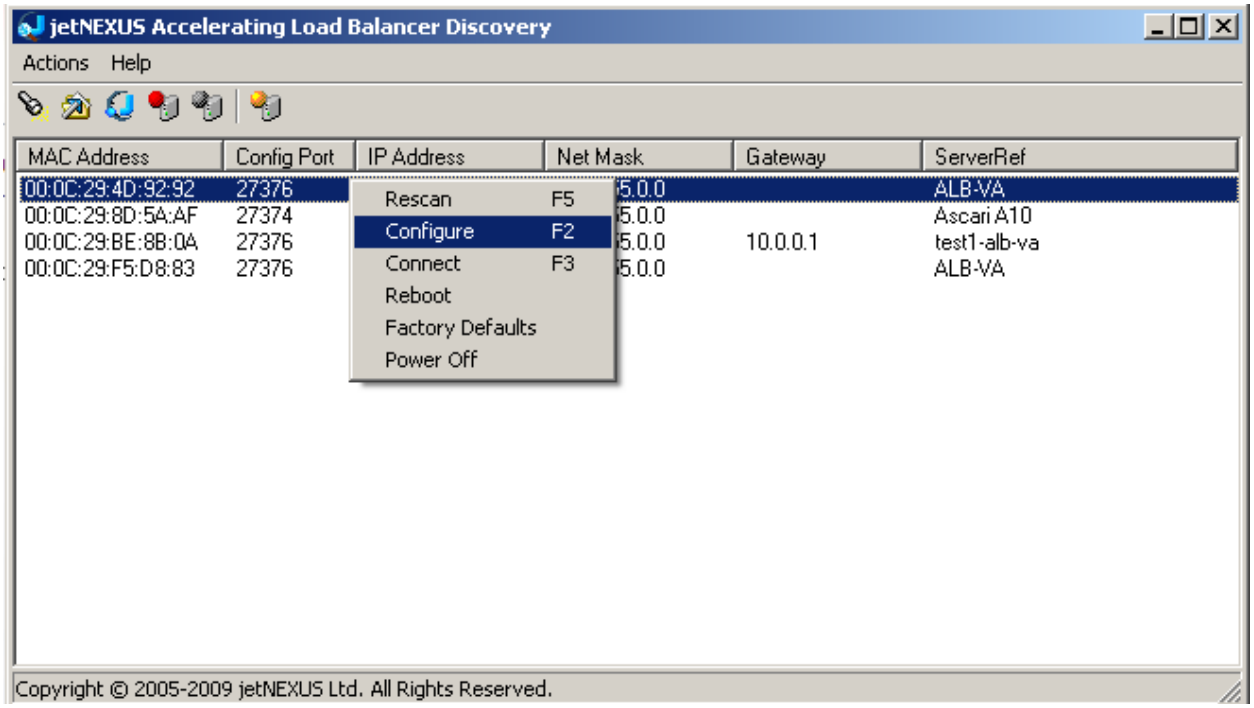
jetNEXUS Discovery

jetNEXUS Discovery is designed to make the initial configuration of the jetNEXUS ALB easy. The application can be installed onto a desktop and will scan the local network for jetNEXUS devices. Once found, essential information such as an initial management IP address can be easily assigned.

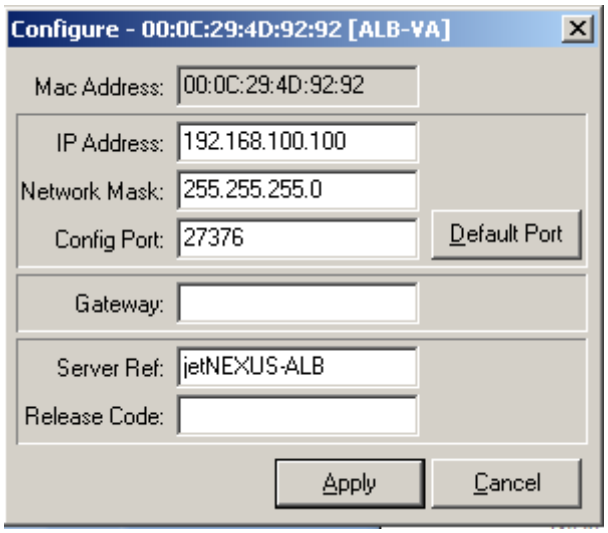
How to use Discovery

Copy the jetNEXUS application onto your desktop and run the installation. After the installation is complete double click on the Discovery Icon to launch the jetNEXUS discovery application.

The jetNEXUS Accelerating Load Balancer Discovery will then open, showing you a list of jetNEXUS appliances in your network:.



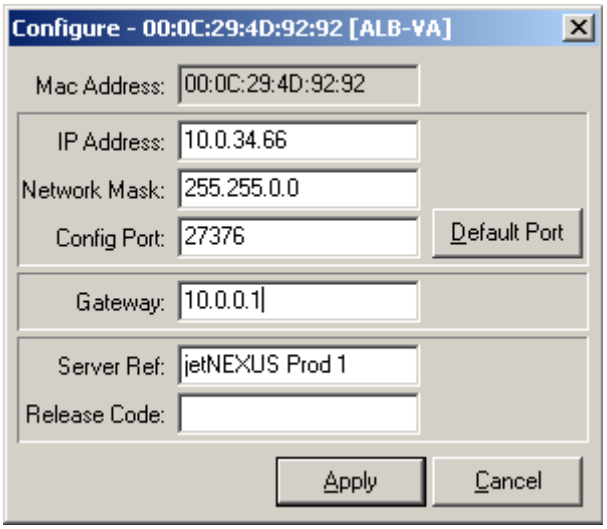
Right click on the on device you would like to configure and select “configure”. A message box like the one below will then pop up:



You will be prompted for the following information:

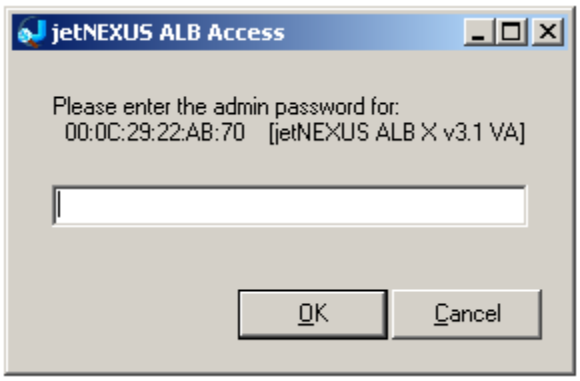
IP Address: The Management IP Address of the device
Network Mask: The network Mask of the Device's management IP
Configuration Port: The configuration port of the secure web interface
Gateway: The Default gateway
Server Ref: A name to identify the device

In this example we have configured the following details:



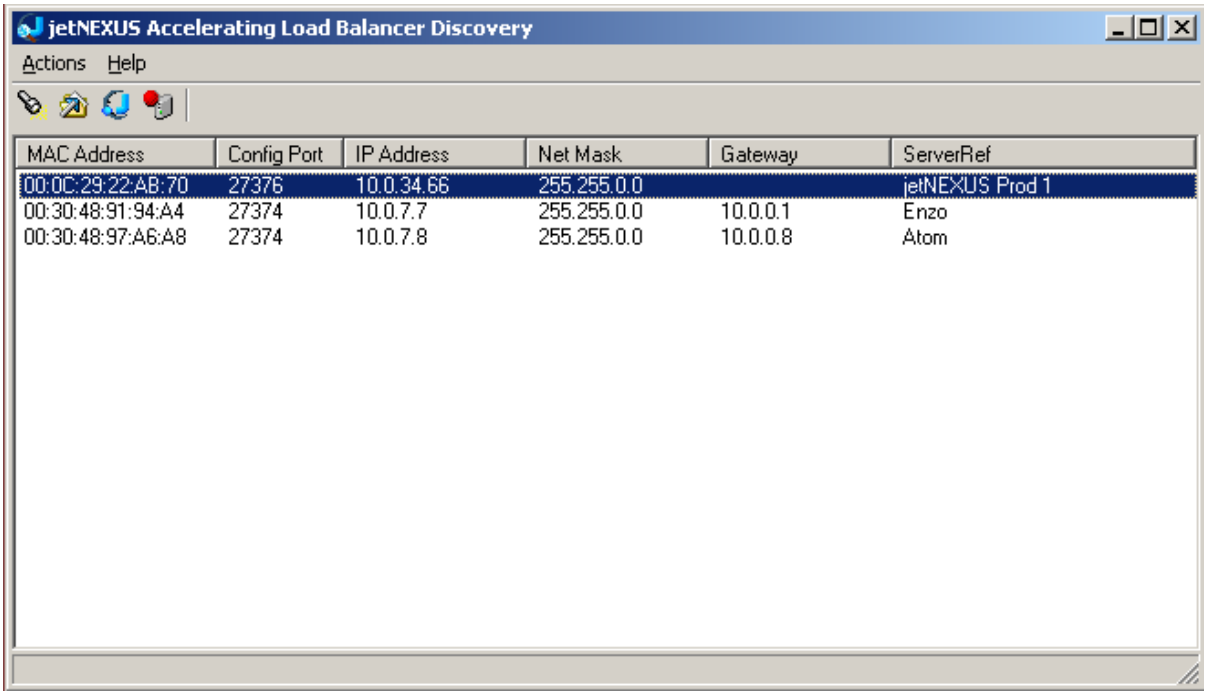
IP Address: 10.0.34.66
Network Mask: 255.255.0.0
Configuration Port: 2736 -Default
Gateway: 10.0.0.1
Server Ref: jetNEXUS Prod 1

Once you click on the apply button you will be prompted for the password:

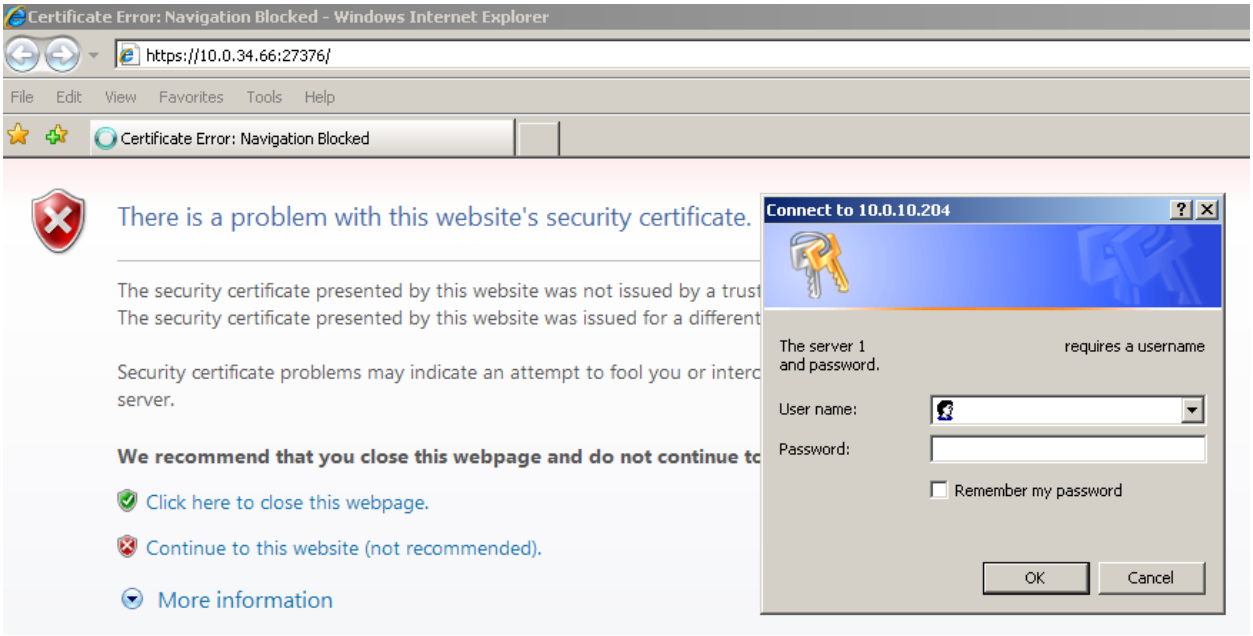


Default password is: jetnexus

Your Configured device with the new IP,Subnet and ServerRef will now show in the discovery screen:



Double click on the ALB you would like to configure and it will load the web admin in a browser:



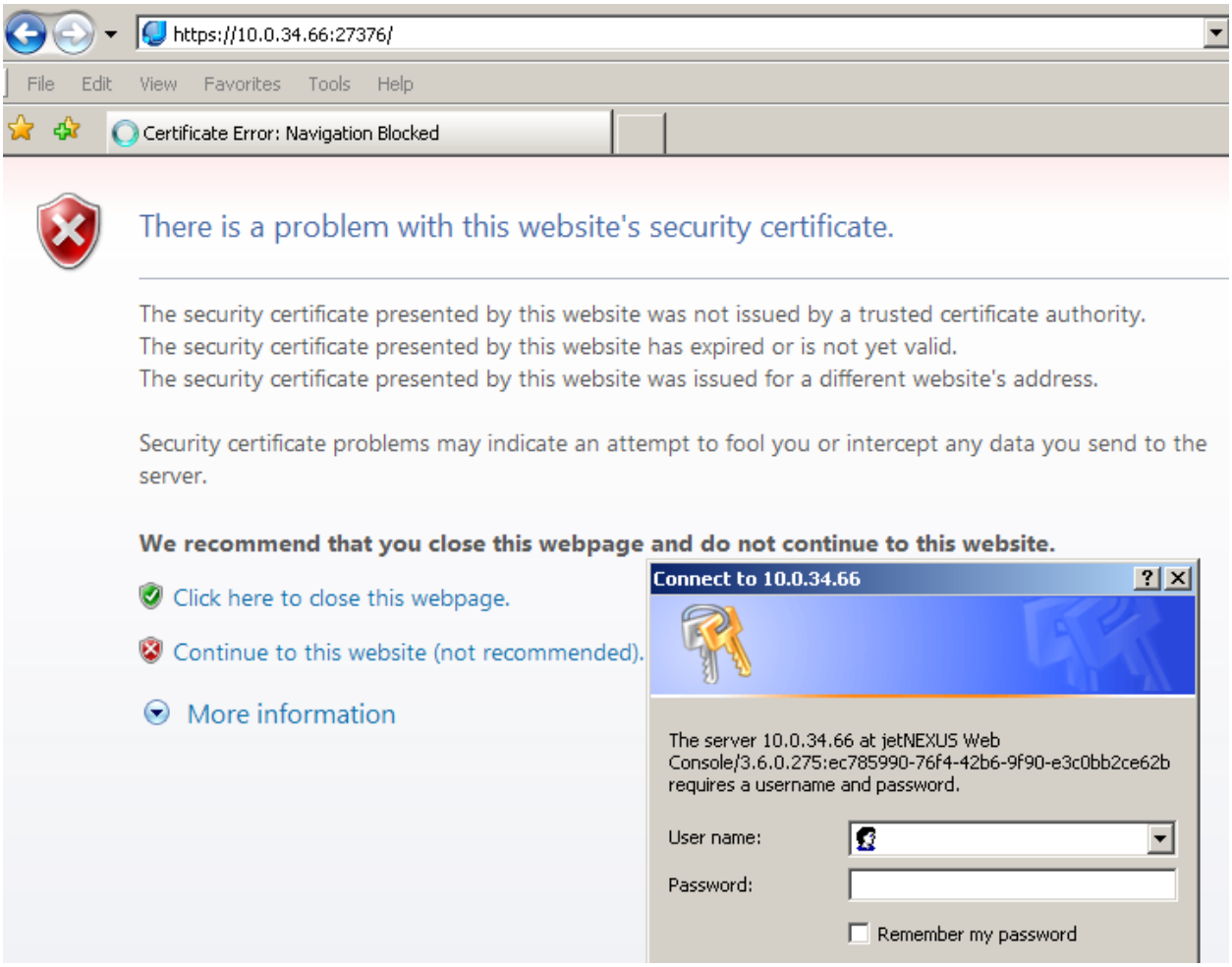
Please go to page 17 to continue the setup of your jetNEXUS ALB via the Graphical Interface.

If you have not chosen to setup your jetNEXUS ALB via jetNEXUS Discovery then please continue to the Basic Configuration web interface.

Basic Configuration web interface

The default web interface can be access via the following IP if it has not been able to contact a DHCP server:

https://192.168.100.100:27376

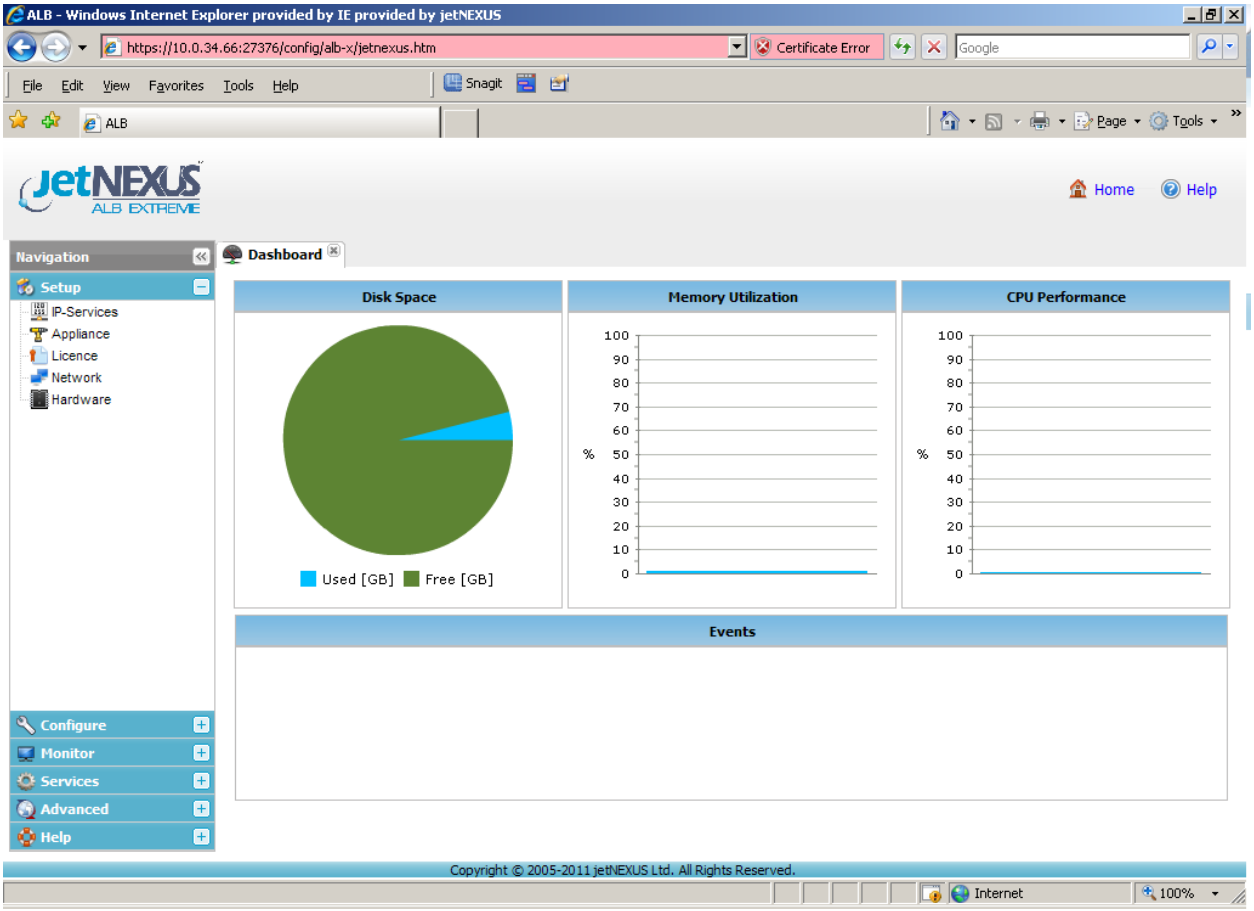


You will be challenged for a username and password:

Username: admin

Password: jetnexus

Once you have logged in you will be presented with the default jetNEXUS screen:



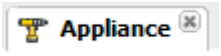
Using the Navigation bar on the left you will be able to access all the options to configure your jetNEXUS ALB.

The Dashboard provides Information on Disk space, Memory Utilization and CPU Performance.

Getting Started

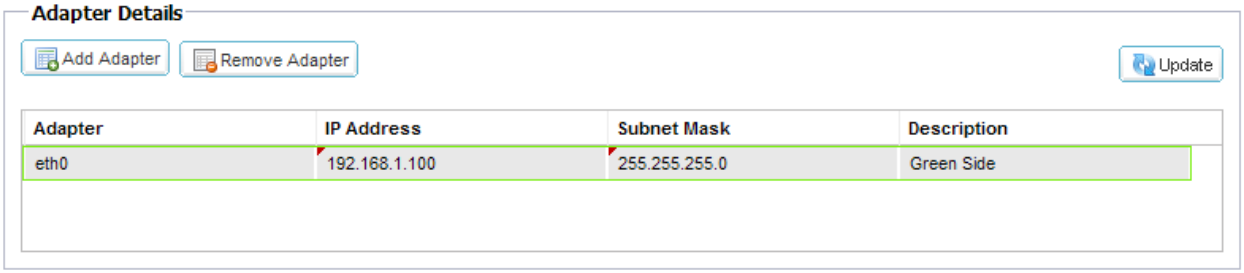
Setting the IP address

The first item to configure when setting up jetNEXUS ALB is the basic networking.

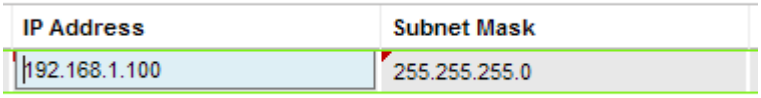
Using the Navigation bar on the left of the web interface go to (Setup →Appliance). This will open the 

tab allowing you to set the IP Address for the unit.

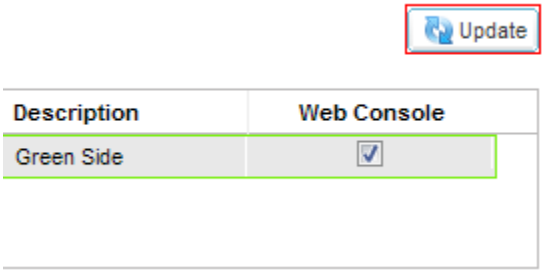
You can now set the network properties:



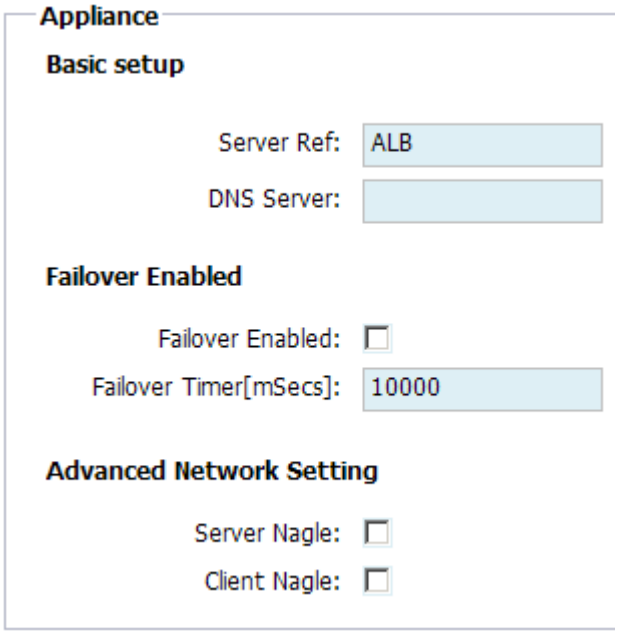
Double click on the IP Address box & Subnet mask to enter the IP and subnet, each section will turn blue allowing you to add IP and subnet information:



Your changes will be highlighted with a red triangle above them, then click on the update button to commit your changes:



You also have to complete the Server Ref naming your appliance information:



Once completed click on the Update button at the bottom right of the page:

jetNEXUS Example

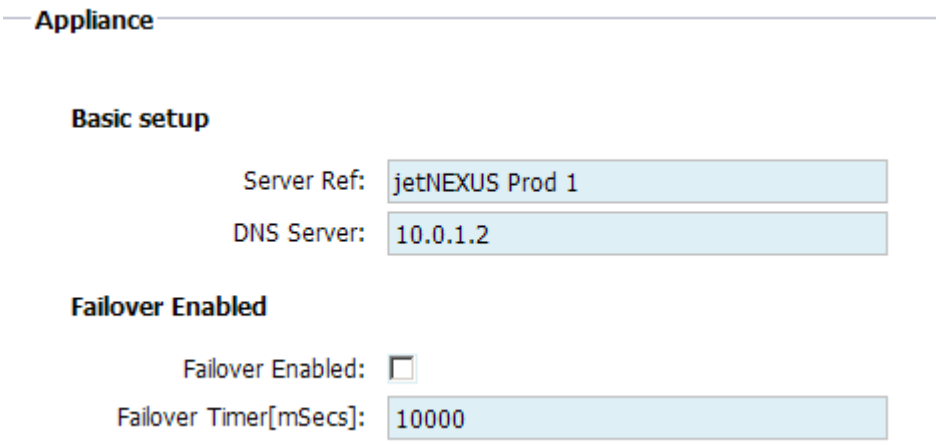
In this example we have configured the details below, and we are using a one-armed configuration Green side only.

Server Ref:	jetNEXUS Prod 1
IP Address:	10.0.34.66
Network Mask:	255.255.0.0
DNS Server:	10.0.1.2

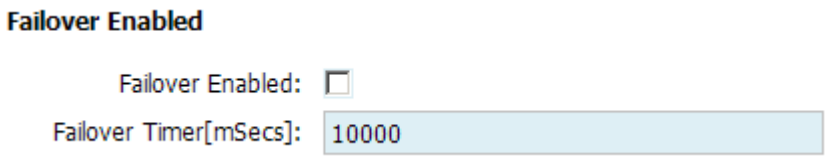
Here we have set the IP address and subnet mask:

Adapter	IP Address	Subnet Mask	Description
eth0	10.0.34.66	255.255.0.0	Green Side

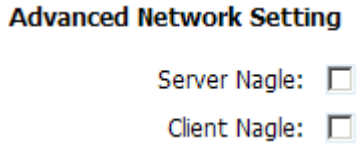
Now set the server ref appliance name and enter your DNS server:



Failover enabled when ticked enables the failover controls; this allows the appliance acts as a as part of a High-Availability cluster. When you have more than one jetNEXUS ALB and require high-availability failover, tick this box. However this will be discussed in more detail later on in this guide:



Server Nagle and Client Nagle can be enabled to pace connections where content is small. These options are not enabled as default, and should only enable on older slower networks:



This is not required for HTTP communications but can be beneficial with some protocols on a Layer 4 channel.

Once all information has been entered please use both update buttons 

You have now configured the Appliance tab.

Setting the Default Route

Using the Navigation bar on the left of the web interface, go to (Setup →Network) this will open the 

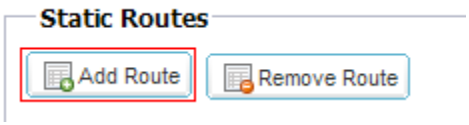
tab allowing you to add the Gateway and Static routing information.

On this screen we configure a default gateway and routing, you must set a Gateway IP Address:

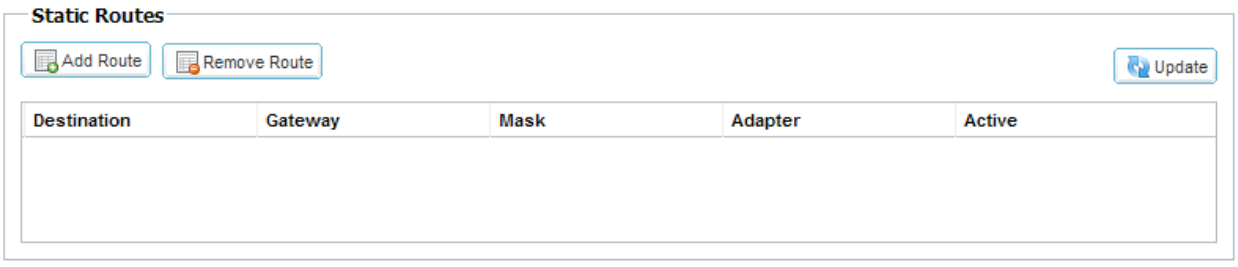
In this example we have configured the Gateway IP of 10.0.0.1 on eth 0 once you have configured your gateway click the update button:

Setting a Static route

Static routes can be added by clicking on the "Add Route" button:

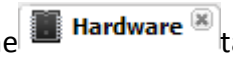


You will need the destination address and mask, the gateway and adapter. Once the details are filled in, click update to action the settings. A tick is shown in the "Active" column when the route is implemented:



You have now configured the Network tab.

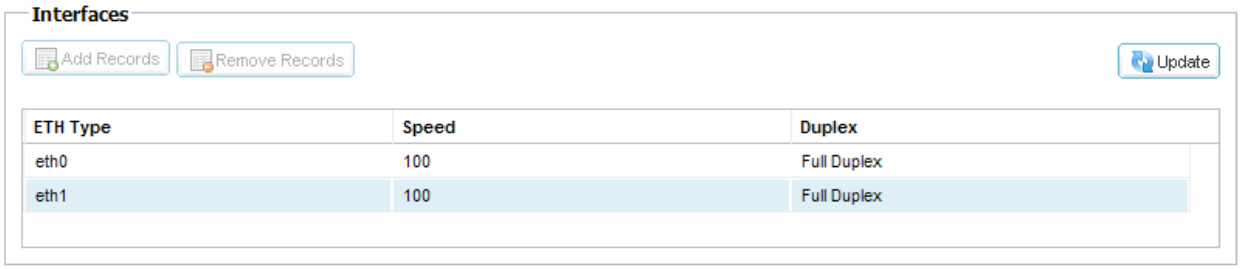
Setting the network speed

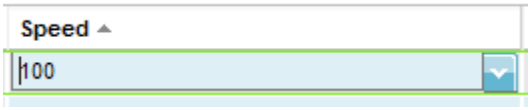
Using the Navigation bar on the left of the web interface, go to (Setup →Hardware) This will open the 

tab allowing you to set the Interface speeds.

The settings on this screen control the network access. The defaults are to fix speed at 100 Mbps and full duplex. This avoids any issue with certain networking devices that have auto-negotiation which re-negotiates too frequently.

The device can support speeds from 10 to 1000, for 1000 this should set to auto/auto. If this does not work, set the exact network hardware values:



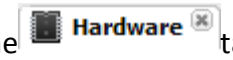
To change the values, click on Speed or Duplex: 

If you have changed any of these settings click the update at the top of the screen.

You have now configured the Hardware tab.

Advanced Networking

Bonding

Using the Navigation bar on the left of the web interface, go to (Setup →Hardware) this will open the 

tab.

What is bonding?

Bonding allows you to aggregate multiple ports into a single group, effectively combining the bandwidth into a single connection. Bonding also allows you to create multi-gigabit pipes to transport traffic through the highest traffic areas of your network.

Bonding Modes

The jetNEXUS ALB supports many different bonding types these are listed below with a brief description.

Balance-rr

The Balance-Round-Robin mode: It transmits packets in sequential order from the first available slave to the last.

Active-backup

The Active/Backup bonding mode: Has one interface will be live and the second interface will be in standby. This secondary interface only becomes active if the active connection on the first interface fails.

Balance-Xor

The XOR bonding mode: Transmits based on (source MAC address XOR'd with destination MAC address) This selects the same slave for each destination Mac address.

Broadcast

The broadcast bonding mode: Transmits everything on all slave interfaces.

802.3ad

The IEEE 802.3ad Dynamic link aggregation bonding mode: Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification.

Balance-tld

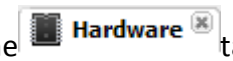
The Adaptive transmit load balancing bonding mode: Provides channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current

slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.

Balance-alb

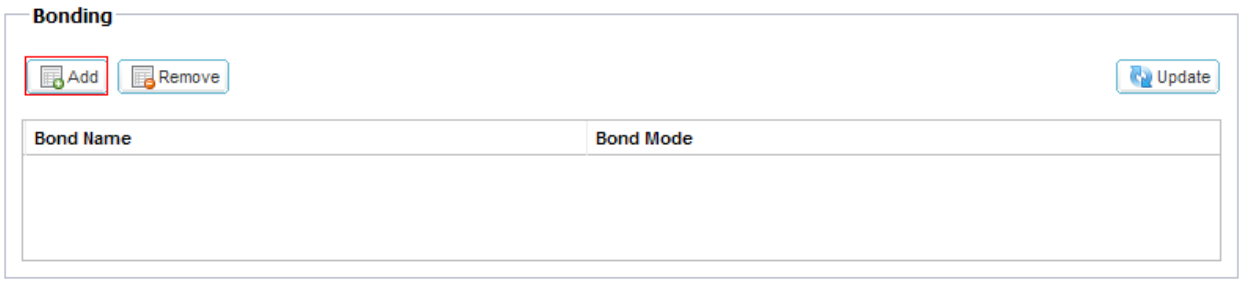
The Adaptive load balancing bonding mode: also includes balance-tlb plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different peers use different hardware addresses for the server.

Configure bonding

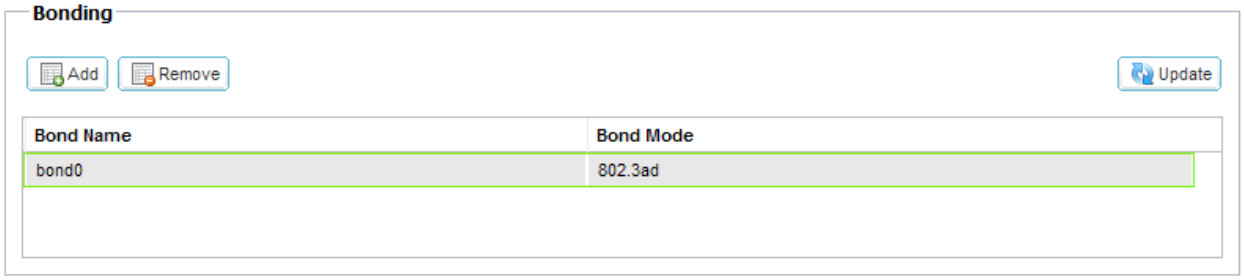
Using the Navigation bar on the left of the web interface, go to (Setup →Hardware) this will open the 

tab.

Bonding is broken down into two sections bonding and interfaces, you will first need to create a Bond. Click on Add button on the bonding section:

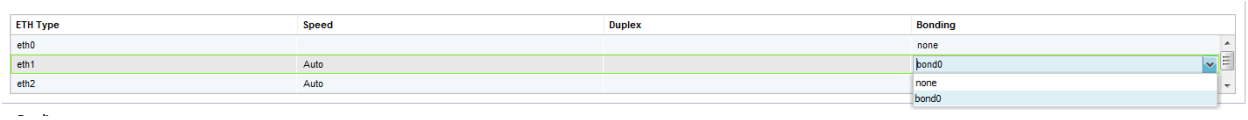


You will then be able to add a new bond and then select your bonding mode:

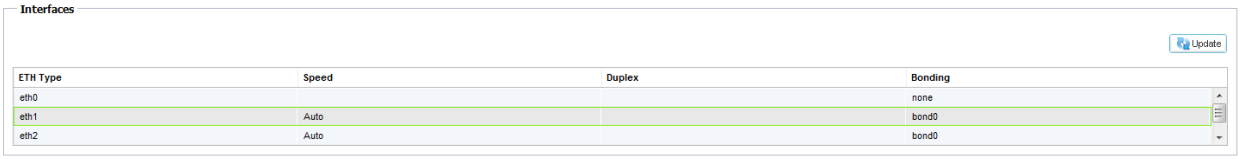


Adding interfaces to the bond

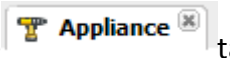
Adding interfaces to a bond, in the example below I will add eth1 and eth2 to bond0:



Both eth1 and eth2 are now part of bond0:

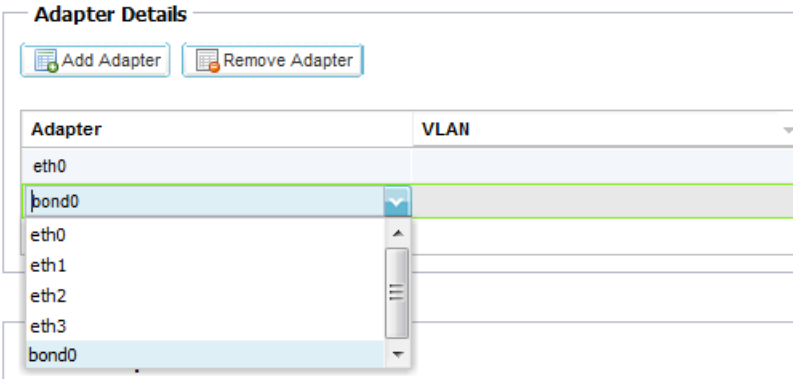


Adding a new bonded adapter

Using the Navigation bar on the left of the web interface, go to (Setup →Appliance) this will open the 

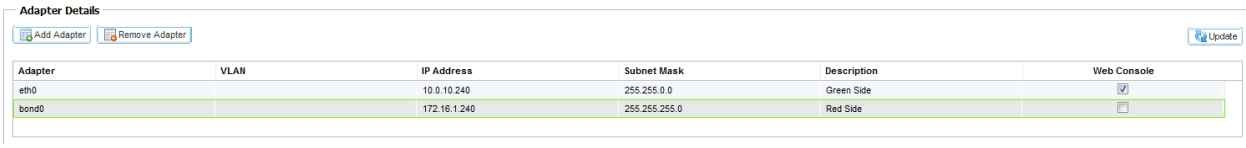
tab.

Click on Add Adapter and select bond0, you will need to configure this with an IP address and subnet mask. In the example I have used 172.16.1.240/24:

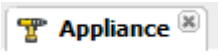


Example:

Bond0 now configured with 172.16.1.240/24:



LAN's

using the Navigation bar on the left of the web interface, go to (Setup →Appliance) this will open the 

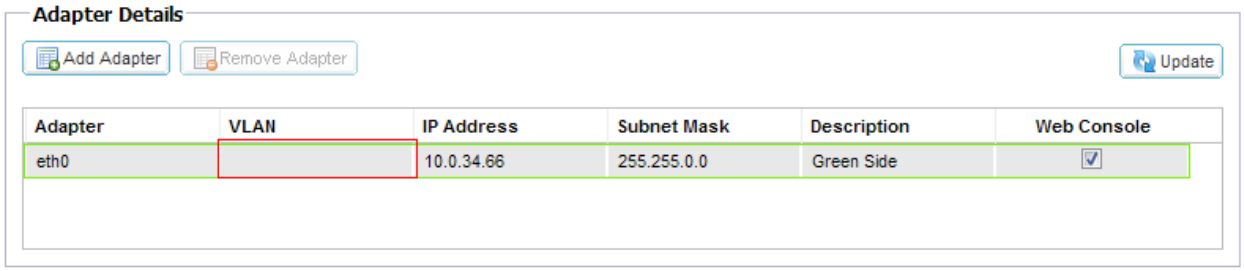
tab.

What is a VLAN?

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location.

Configure a VLAN

On the Adapter settings screen you have the ability to add VLAN information into the VLAN box highlighted below:



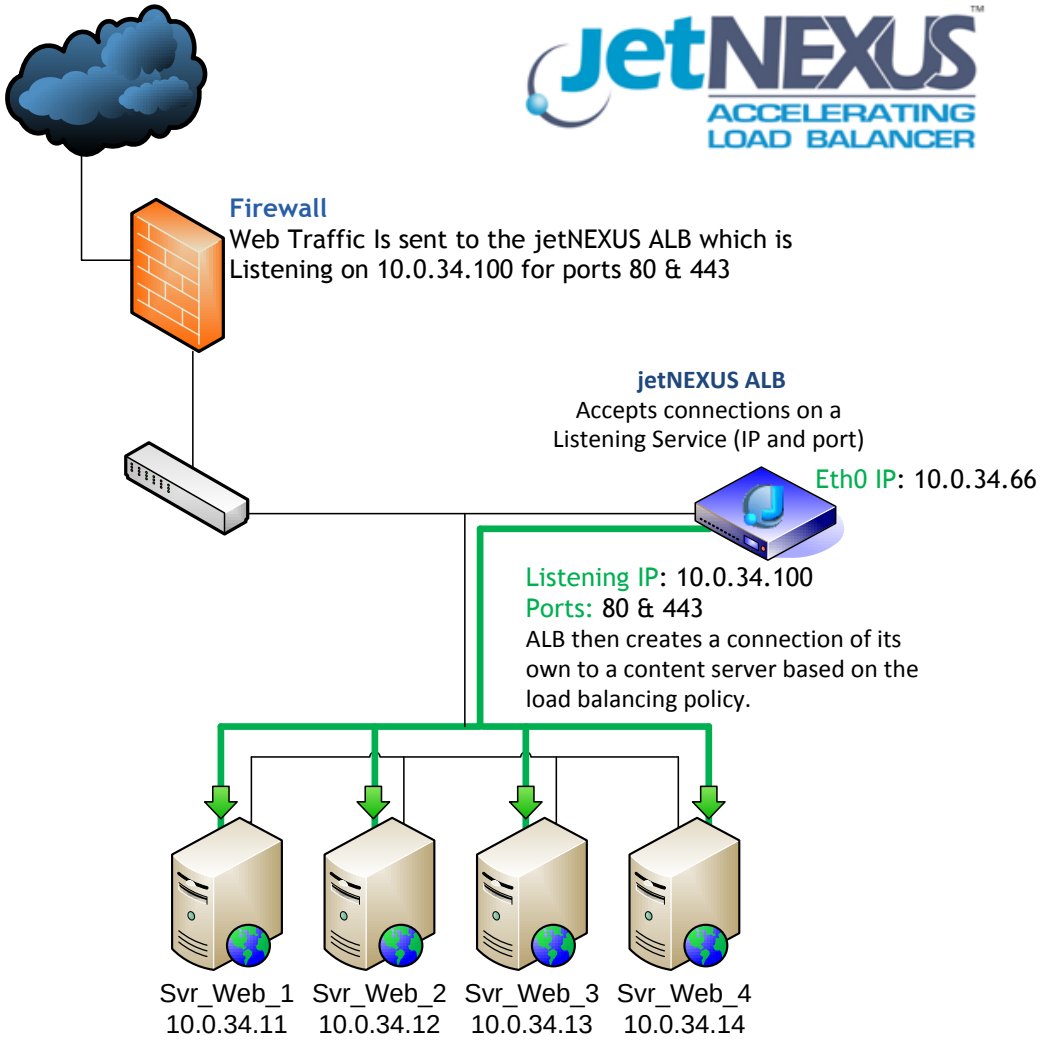
ALB Implementation

There are two fundamental ways to deploy jetNEXUS Accelerating Load Balancer.

Single network interface configuration

Enabling only the eth0 (single network interface) and installing your jetNEXUS ALB into the same network as your Web server/Applications servers flat network; this is suitable for most scenarios. All inbound and outbound traffic passes over this single network interface.

jetNEXUS ALB accepts connections on a listening Channel (The combination of IP address and port) and holds this. It then creates a connection of its own to a backend server based on a load balancing policy. When it gets the required data from the server, the jetNEXUS ALB then sends it on to the client. In this configuration the web management traffic also goes over the single interface.

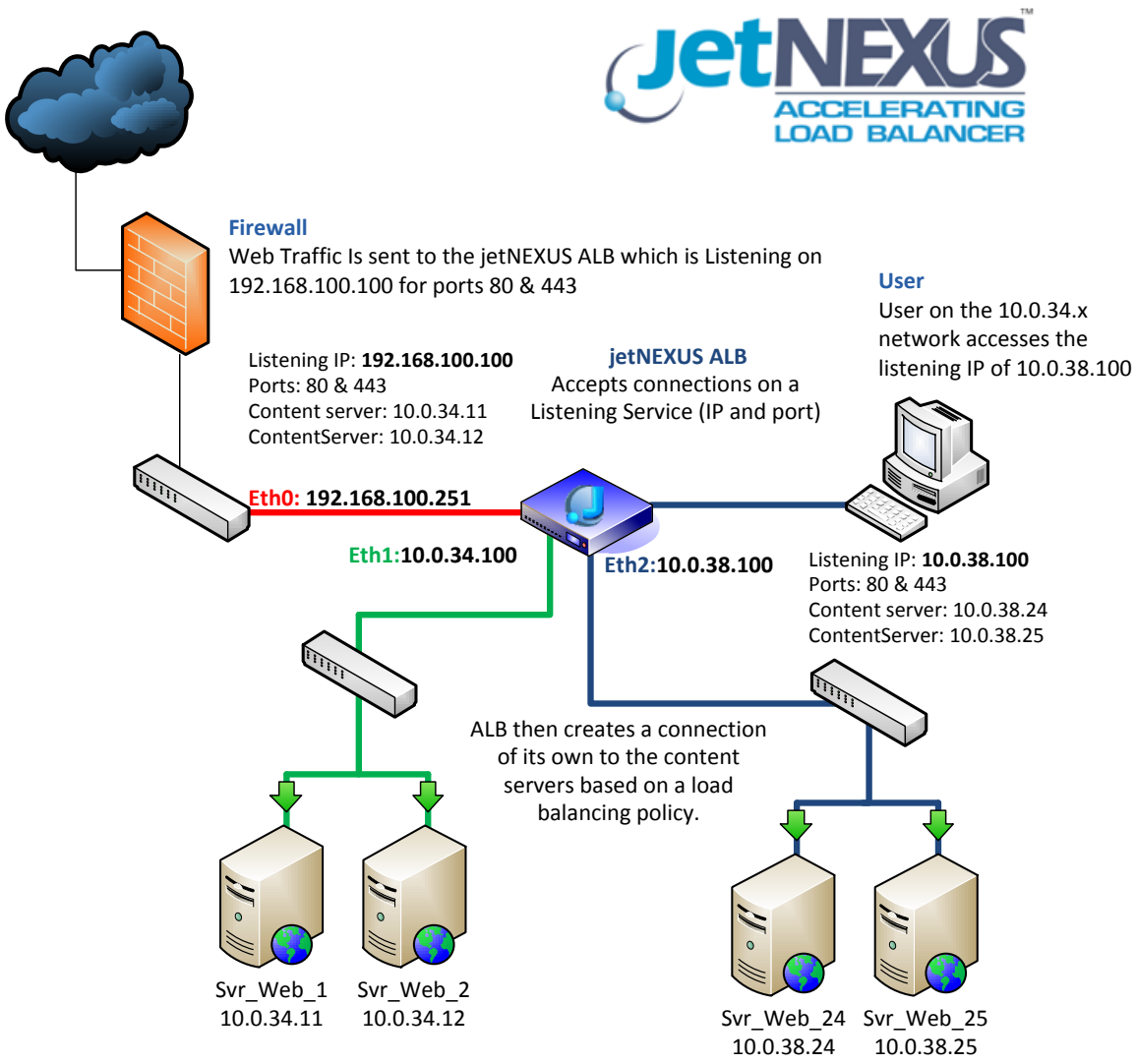


Multi network interface configuration

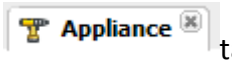
Enabling the Eth0 interface, and any another interface Eth1/Eth2 &Eth3 etc. The jetNEXUS devices can proxy the traffic between any of the new network interfaces. This is suitable for larger scenarios where network segmentations between web services are needed.

jetNEXUS ALB accepts connections on a listening Channel (The combination of IP address and port) on any of the following interfaces Eth0/Eth1/Eth2 &Eth3 and holds this information. It then creates a connection of its own to a backend server based on a load balancing policy.

In a Multi Network configuration all traffic between the client and the jetNEXUS ALB can go over any interface you specify in your channel configuration as the listening IP. All traffic between the jetNEXUS ALB and the content server's will go over whatever interface the content server's IP is in.

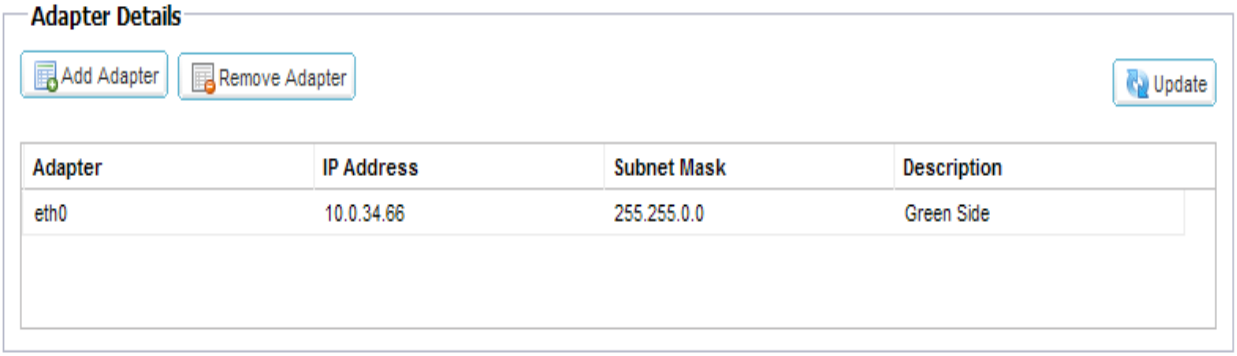


Deploying a single network interface configuration

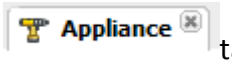
Using the Navigation bar on the left of the web interface, go to (Setup →Appliance) this will open the 

tab allowing you to access the adapter settings.

The example below shows that we only have the address of 10.0.34.66 assigned to eth0 and this shows that the device is currently running in a single network interface configuration:

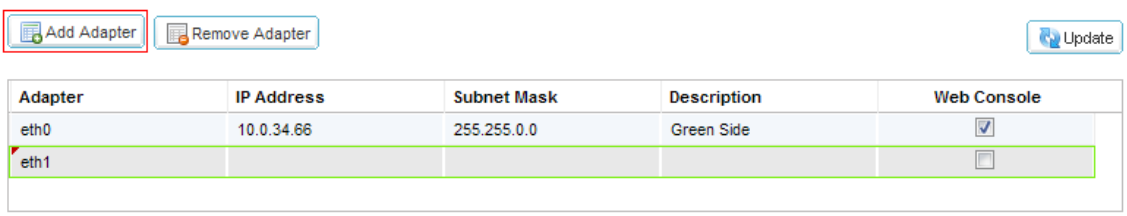


Deploying a multiple network interface configuration

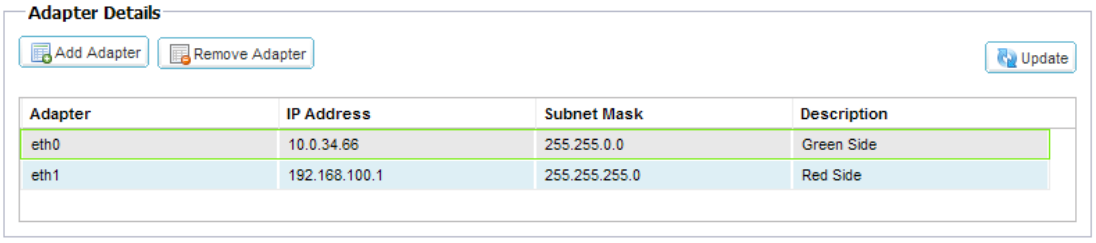
Using the Navigation bar on the left of the web interface, go to (Setup →Appliance) this will open the 

tab allowing you to access the adapter settings.

The example below shows that we only have the address of 10.0.34.66 assigned to eth0 by clicking on the “Add Adapter”, we can now add the details for the eth1 interface:



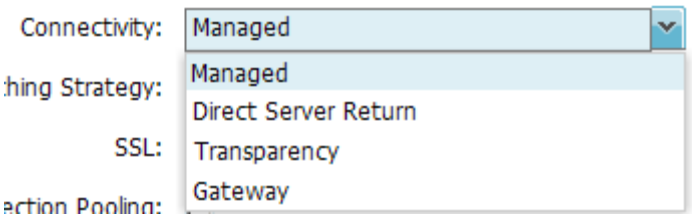
Fill in the address and subnet mask for the second (eth1) adapter. Once completed click on Update and ALB will raise the interface on the eth1 adapter:



jetNEXUS Connectivity modes

You can configure your Channel IP services to run in the 4 connectivity modes below, each mode is detailed below.

Once you have configured a Channel you will be able to access the Connectivity options:



Managed

This is the default setting for jetNEXUS and works at, Layer7 with compression and Caching and also at layer4 without caching and compression. In this mode the jetNEXUS acts as a proxy and becomes the source address seen on the content servers.

How it works

- - Client sends a request to the jetNEXUS
- - Request received by jetNEXUS
- - Request routed to content servers
- - Response sent to jetNEXUS
- - jetNEXUS responds directly to client

Direct Server Return

Direct Server Return, or DSR as it's widely known (DR – Direct Routing in some circles) allows the server behind the load balancer to respond directly to the client bypassing the jetNEXUS on the response. DSR is suitable for using with layer 4 load balancing only therefore Caching and Compression are not available when enabled.

Layer 7 load balancing with this method will not work therefore there is no persistence support other than source IP. SSL/TLS load balancing with this method is not ideal as there is only source IP persistence support.

How it works

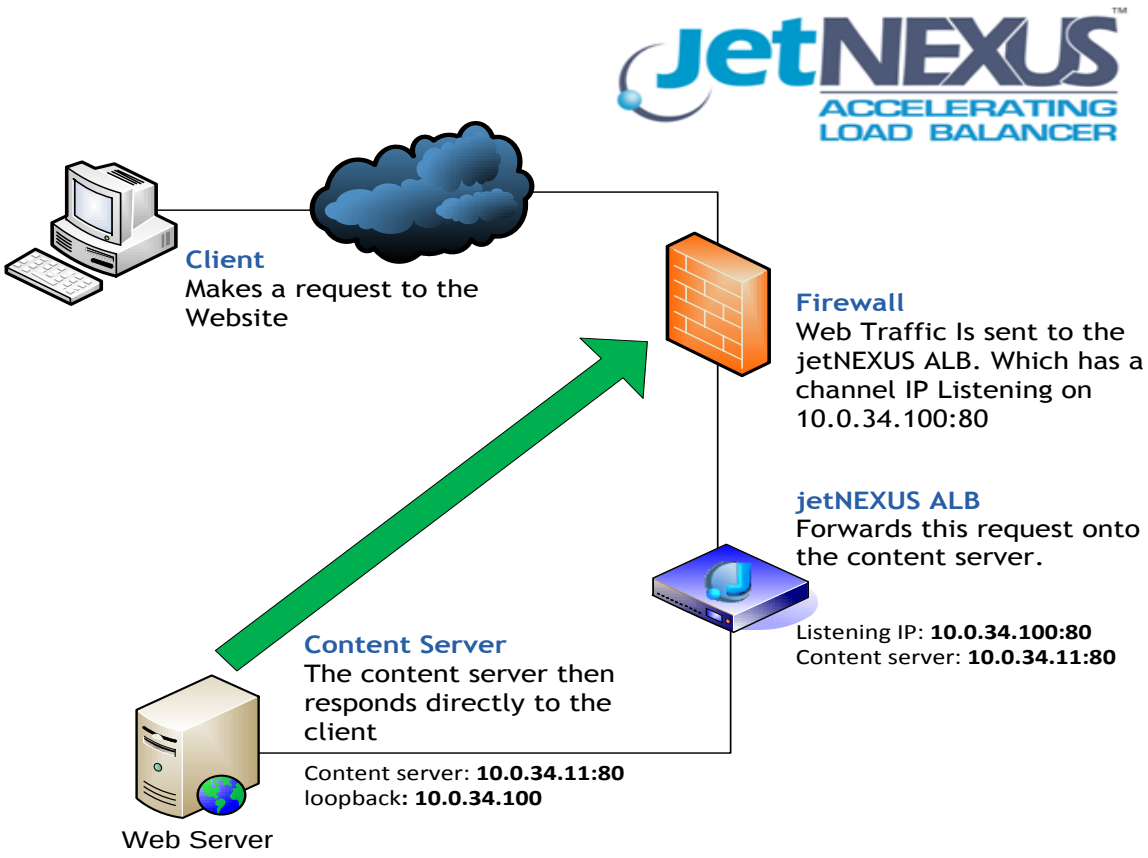
- - Client sends a request to the jetNEXUS
- - Request received by jetNEXUS

- - Request routed to content servers
- - Response sent directly to client without passing through JetNEXUS

Configuration

Your content server will need to be configured, to have a new Alias added to the loopback interface. This Alias needs to be the same as the channel IP on your jetNEXUS, which you have configured DSR on.

Diagram



Transparency

Transparency is suitable for layer 4 load balancing only, Caching and Compression are not available when transparency is enabled. Transparency is used when you need the source address of the client making the request.

How it works

- - Client sends a request to the jetNEXUS
- - Request is received by jetNEXUS

- - MAC changed Request routed to content servers
- - Response sent to jetNEXUS
- - jetNEXUS routes the response to the client

Configuration

Content servers need to be configured to use the jetNEXUS as their default gateway.

Gateway

Gateway mode allows you to route all traffic through the jetNEXUS, this allows traffic from the content servers to be routed via the jetNEXUS to other networks via the interfaces on the jetNEXUS unit. Using the device as a gateway device for content servers should be used when running in multi interface mode.

How it works

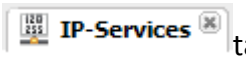
- - Client sends a request to the jetNEXUS
- - Request is received by jetNEXUS
- - Request sent to content servers
- - Response sent to jetNEXUS
- - jetNEXUS routes the response to the client

Configuration

Content servers need to be configured to use the jetNEXUS as their default gateway.

Configuring a channel service

Adding a load balanced service

Using the Navigation bar on the left of the web interface, go to (Setup →IP Services) this will open the 

tab allowing you to access the IP Services options.

The IP service page is spilt into 3 sections; each section must be completed after each other to enable a channel IP.

Channel Details

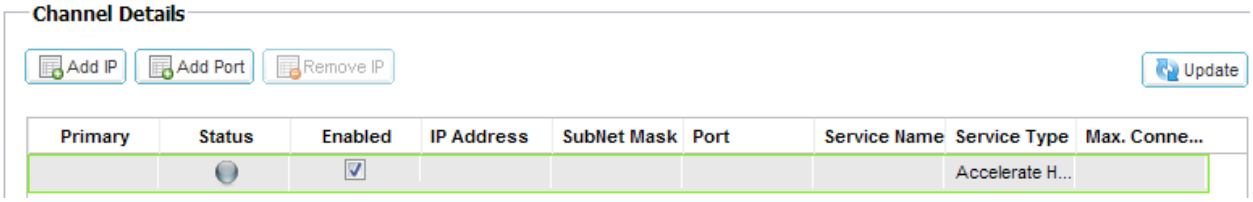
Destination

Actions

Setup Channel Details

To configure a channel click the “Add IP” button:

This will now add a black Channel IP service ready for configuration:



Channel descriptions

Each Channel has a number of configuration options that are described below.

Primary:
This is used to configure a channel as a primary of standby channel – More information can be found on this in the chapter on failover.

IP Address:
The Virtual IP for the channel.

Subnet Mask:
The Subnet mask for the virtual IP.

Port:
The port for the channel to listen on.

Service Name:

A useful name to describe your service.

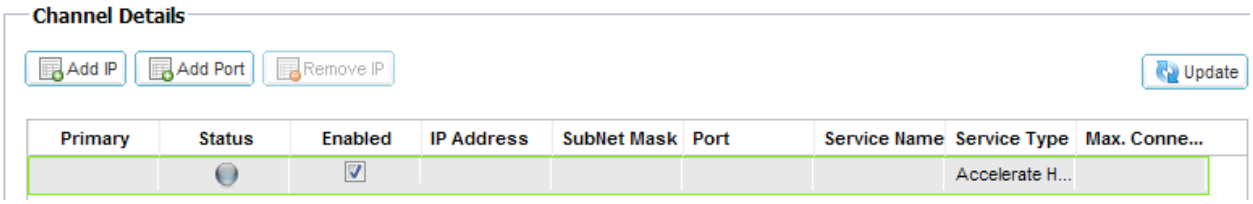
Service Type:

Method is the protocol - There are currently 4 options:

- **Accelerate HTTP**- Layer 7 with compression
- **HTTP** - Layer 7 no compression
- **FTP**
- **Layer4**-Layer 4

Configuring a new channel

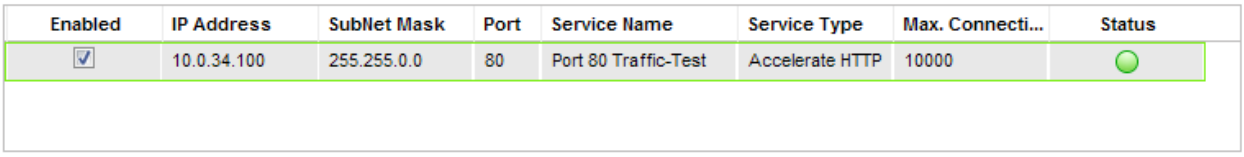
To configure the new click the “Add IP” button:



In this example we will configure the following IP details, based on a One-Armed Configuration.

Channel details:

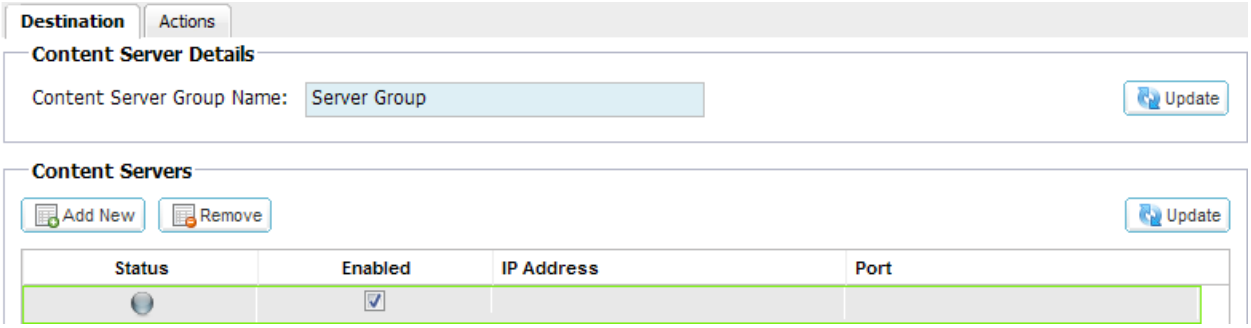
IP Address:	10.0.34.100
Subnet Mask:	255.255.0.0
Port:	80
Service Name:	Port 80 Traffic-Test
Service Type:	Accelerate HTTP
Max connections:	10000



You have now configured the Channel Details.

Setup Destination Details

When you add a channel IP the first content server is added for you, this blank field allows you to add the IP Address and Port of your backend server:



Content Server descriptions

Configuration options are described below.

Content Server Group Name:

You can specify a name for the content servers.

Status

This service indication light will show if the backend server is available (see service indication lights later in this manual).

Enabled

This tick box allows you to enable or disable a backend server from the channel.

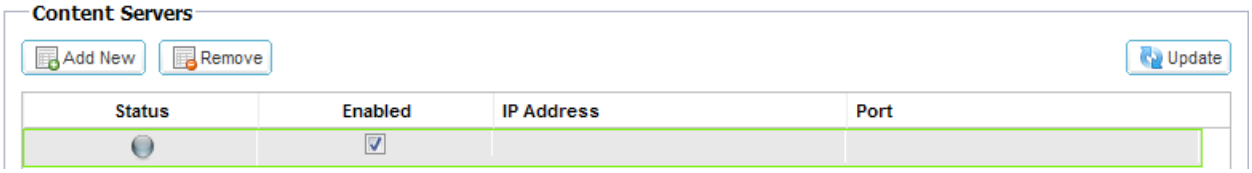
IP Address

The IP Address of your backend content server.

Port

The port that your backend content server is listening on.

Configuring a new Content server



In this example we will configure the following Content server details

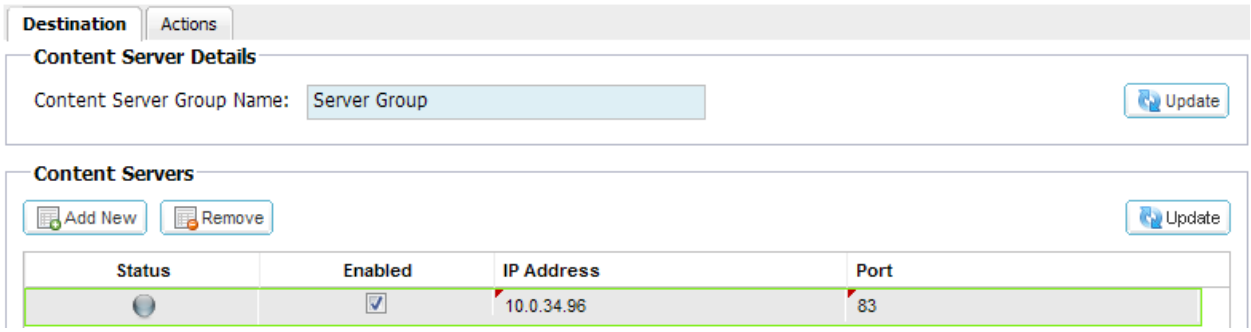
Destination:

Connection Server Group Name: Server Group

Enabled Ticked

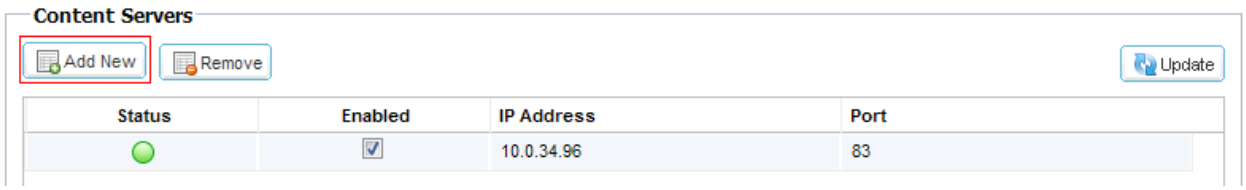
IP Address: 10.0.34.96

Port: 83

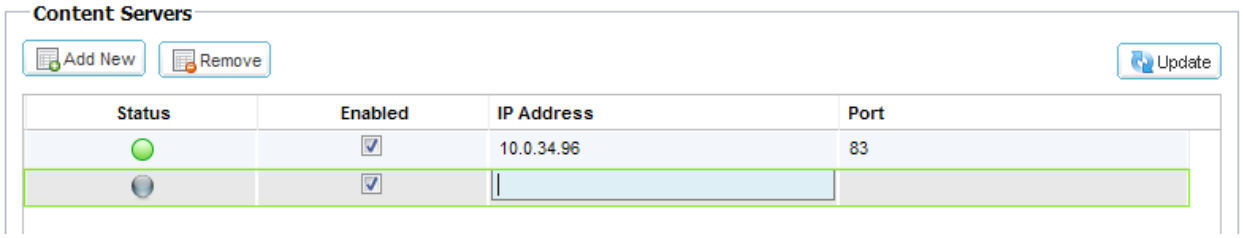


Adding additional Content servers

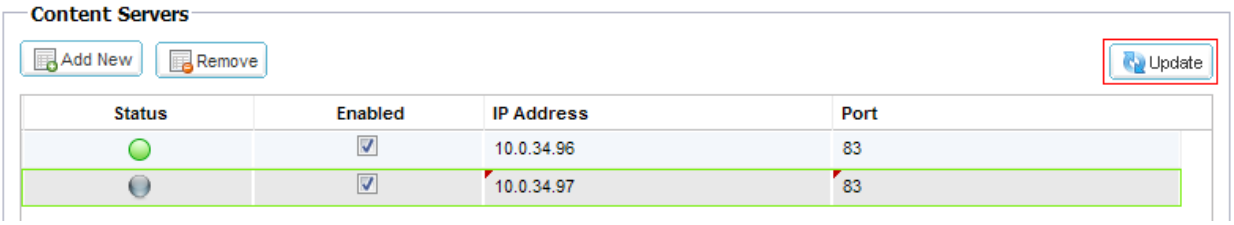
To add additional content servers click on the "Add New" button to add a server:



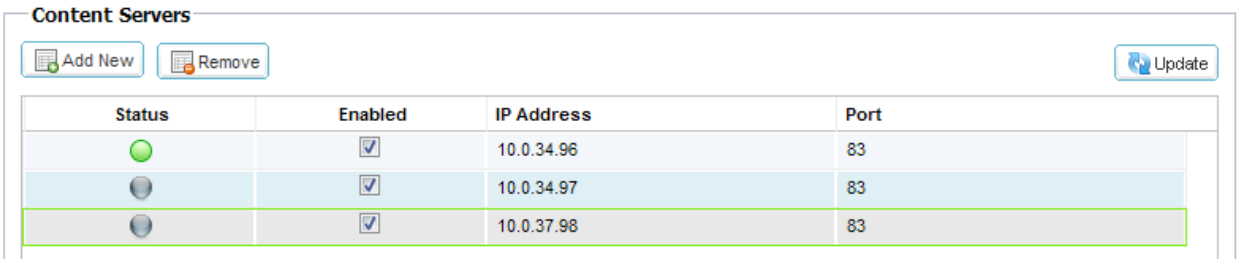
You can now add your additional content servers:



Click on the Update button next to the "Add Content server" this enables the new content server:



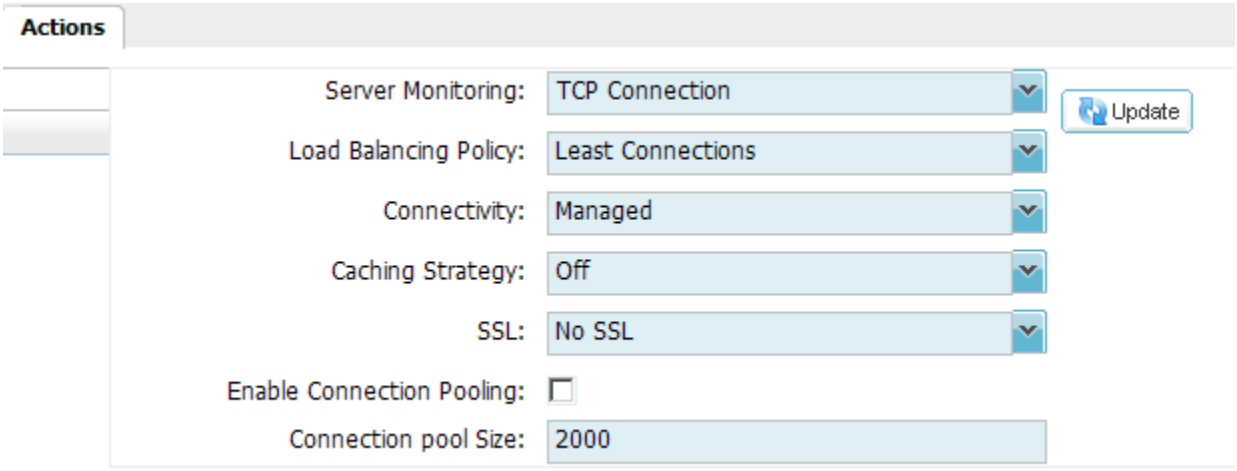
In the example below I have added my 3 content servers to my load balanced channel:



You have now configured the Content server Details.

Setup Actions

The default options for Actions allow you to select several different options these are detailed below:



Action descriptions

Server Monitoring

There are several different monitoring types are defaults are below:

- Ping/ICMP Echo
- TCP Connection
- 200 OK

Load Balancing Policy

There are several different Load Balancing methods they are listed below, they will be covered in more detail later in this manual:

- Least Connections
- Cookie Based
- Round Robin
- IP Based
- IP List Based
- Classic ASP Session Cookie
- ASP.NET Session Cookie
- JSP Session Cookie
- JAX-WS Session Cookie
- PHP Session Cookie

Connectivity

There are several different modes that the ALB can run in the default is managed:

- Managed
- Direct Server Return
- Transparency
- Gateway

Caching Strategy

There are 3 caching strategy's these are listed below

Select SSL Certificate

Once you have added a SSL Certificate then you will be able to see your certificate. The default is to NO SSL if you have no certificates.

Enable Connection pooling

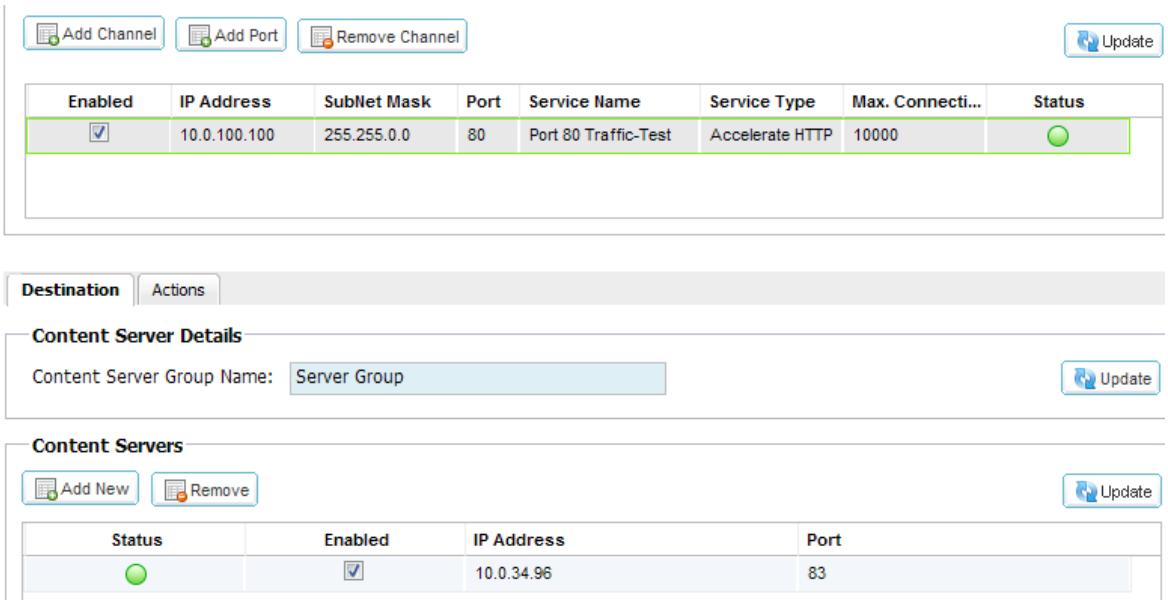
Maintains connections so they can be reused when future requests to the backend nodes are requested.

Connection Pool Size

This is a size limit allowing you to modify the size of the pool

Our new channel has been setup, click on the update buttons in each section to save the new configuration.

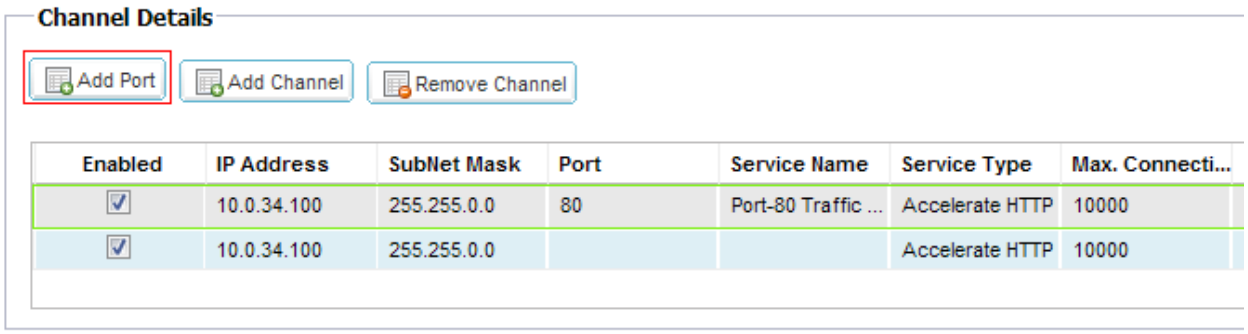
Our Channel has now been configured correctly; the Listening IP and Connection server IP are now shown as Green:



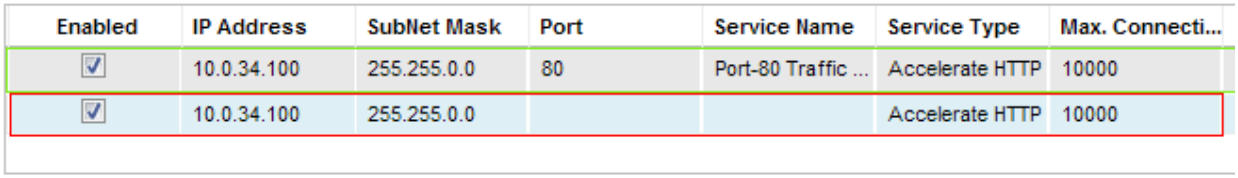
You have now configured an IP Service.

Adding another service on the same channel

To set up another service on the same IP address and a different port click the “Add Port”:



This will add another grouping of settings similar to the first set. This time you don’t need to specify the listening IP or subnet as it has already been added:



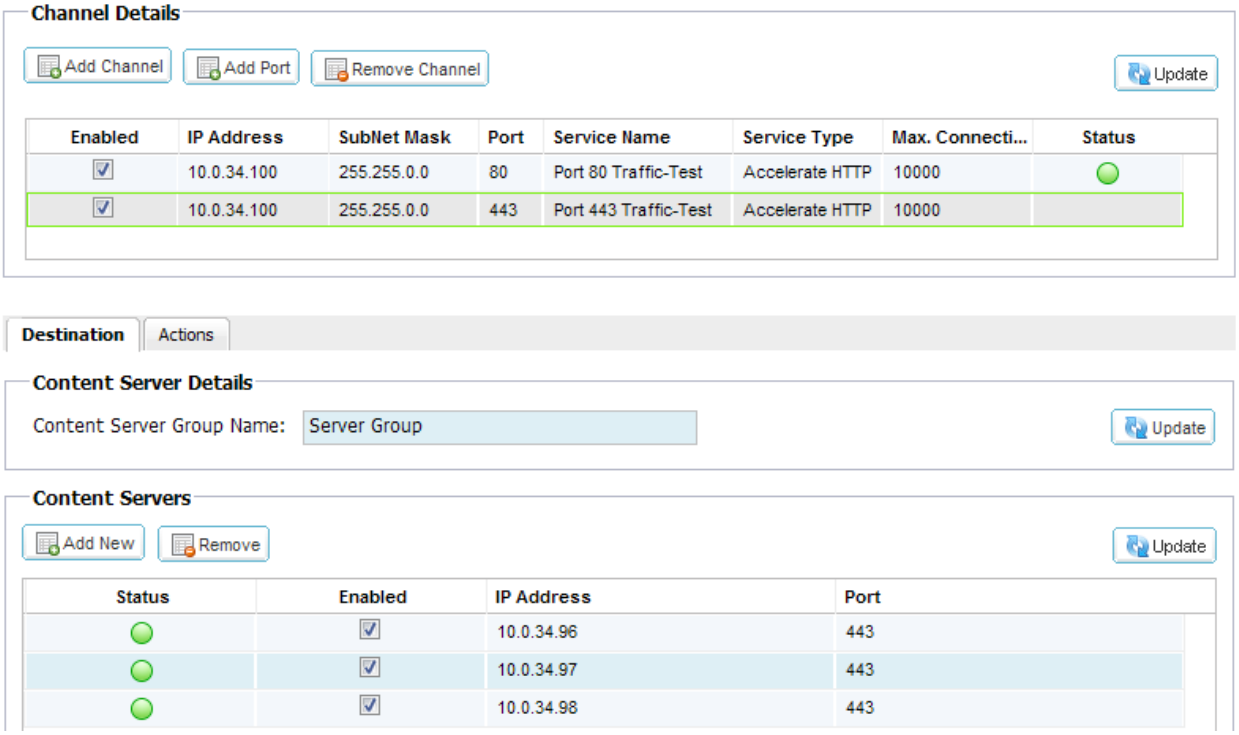
This now allows you to set up the new port and a set of web servers. These can be the same as, or different from the first ones.

Example:

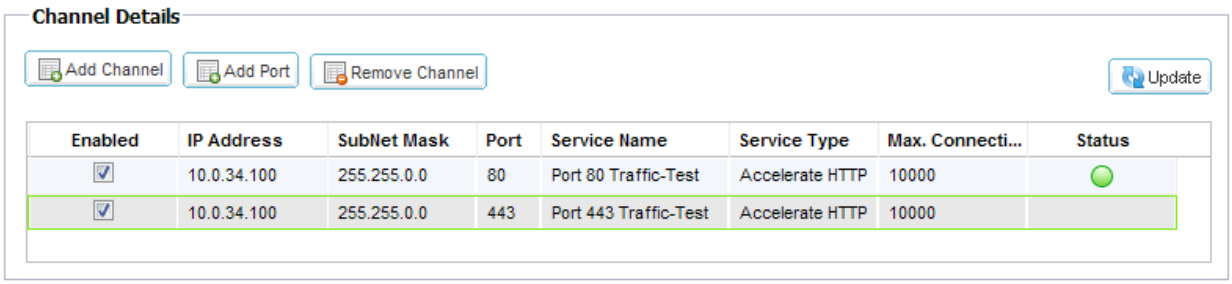
IP Address:	**10.0.34.100***
Subnet mask:	**255.255.0.0***
Port:	443
Service Type:	Accelerate HTTP
Max. Connections:	10000
Content Server group Name:	Traffic-Test
Content Servers	10.0.34.96
	10.0.34.97
	10.0.34.98
Port:	443

***(Automatically propagated from the first rule)**

In the example below I have added my 3 content servers to my existing load balanced channel but this time for port 443:



The original channel is still in place and active, these rules now services port 80 & 443 to the content servers. Via the virtual IP of 10.0.34.100:

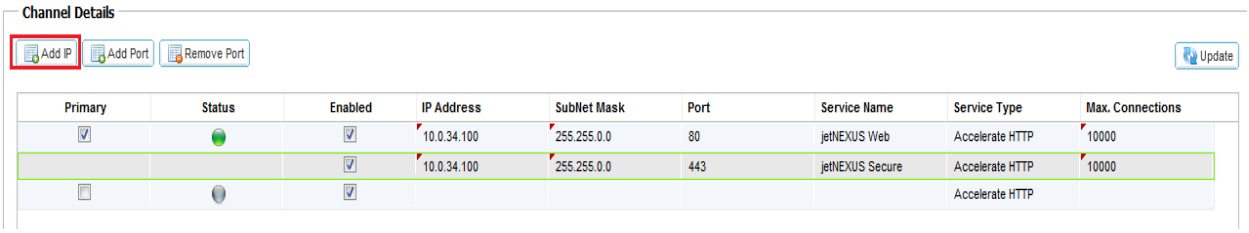


You have now configured a new channel IP Service port.

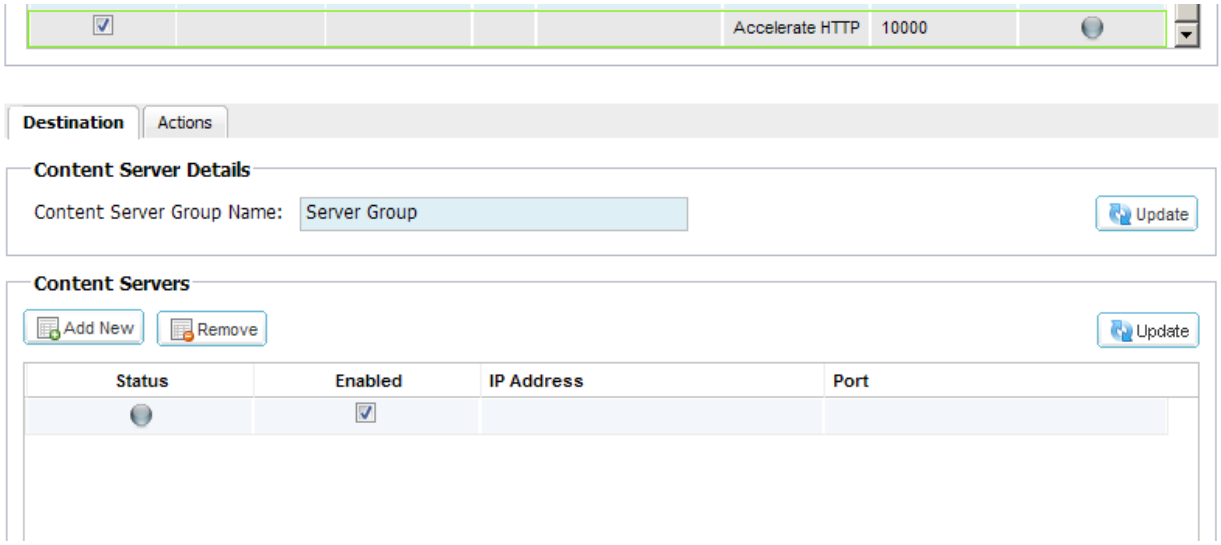
Adding an additional channel IP

To add another listening IP addresses, click on the “Add IP” button:

This will bring up a new section including the option for the second IP address and port:



You can now type in the Details for your new channel IP service and configure the content servers and actions for this new service:



Channel Status lights

There are two groups of status lights: One for the Channel and multiple for the content servers.

Application server and or channel are providing service

Application server and or channel is NOT providing service

Channel is in standby as the primary is serving, or server is offline

Secondary channel is assessing primary service state

Not in use

Unit not licensed

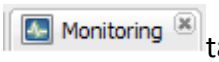
Server Health Monitoring

When in a normal running situation the ALB will initiate active connections to the applications servers when a user makes a request. In addition to this the ALB can also perform active server monitoring. This active monitoring can be configured to perform more advanced test to validate if the web server can provide service. These tests occur irrespective of any load.

The choices for tests are as follows:

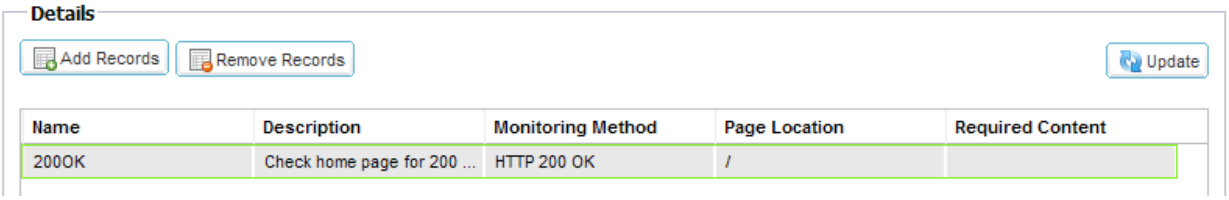
None	-	No active monitoring
Ping	-	Perform a ping
HTTP 200 OK	-	Check the response code form the web server is 200 OK
HTTP Response	-	Check the body of the response for a particular string

Configuring Server Health Monitoring

Using the Navigation bar on the left of the web interface, go to (Configure →monitoring) this will open the 

tab allowing you to access the monitoring options.

To add a new monitor you will be presented with the following screen:



You will need to fill in the Content Server Monitoring method screen with the following information.

Name

Give the new method a useful name

Description

Give the new method a useful description

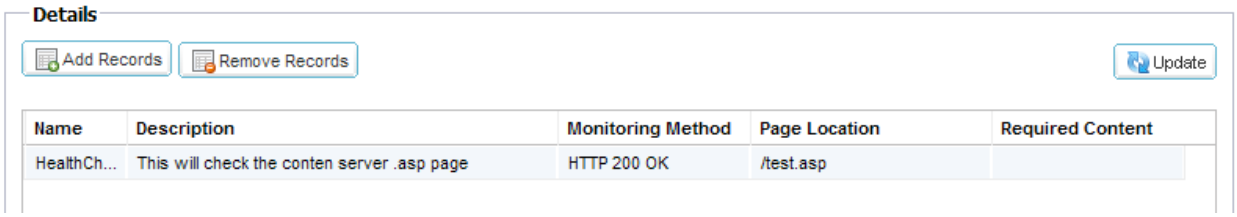
Monitoring Method

Type of Monitoring HTTP 200 ok or HTTP Response

Page location

The page location is the page that you would like to test from the ALB

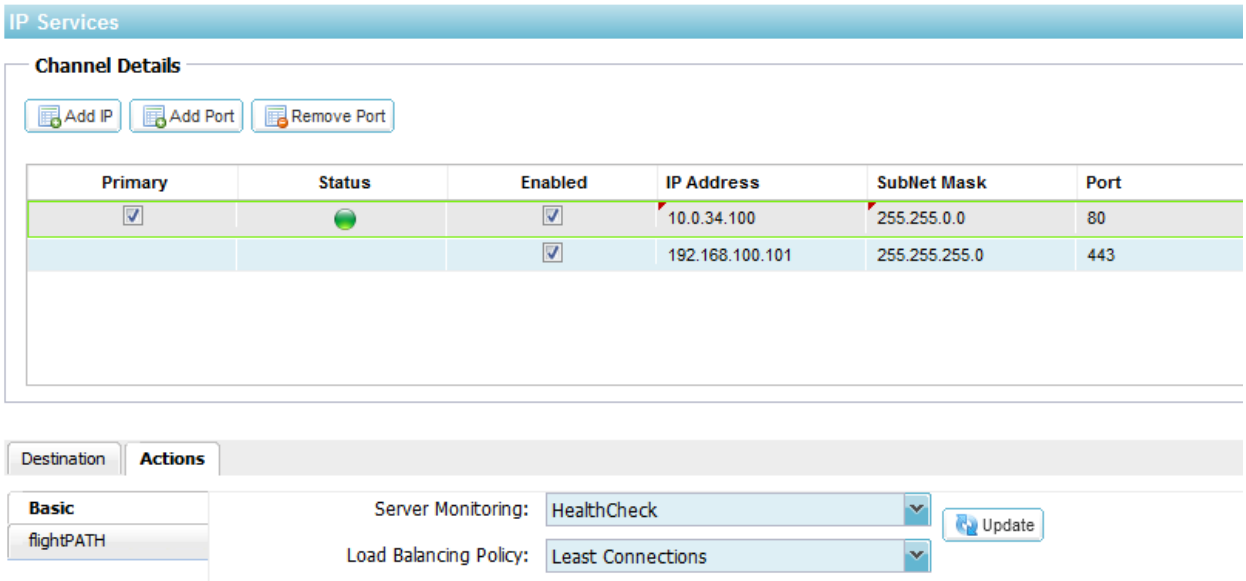
In the example below I have configured a health monitor using HTTP Response to check for a test.asp page on my content servers:



Next we need to apply this new method to our service. Go back to the IP services screen and select the channel service you want this monitor enabled on.

Example

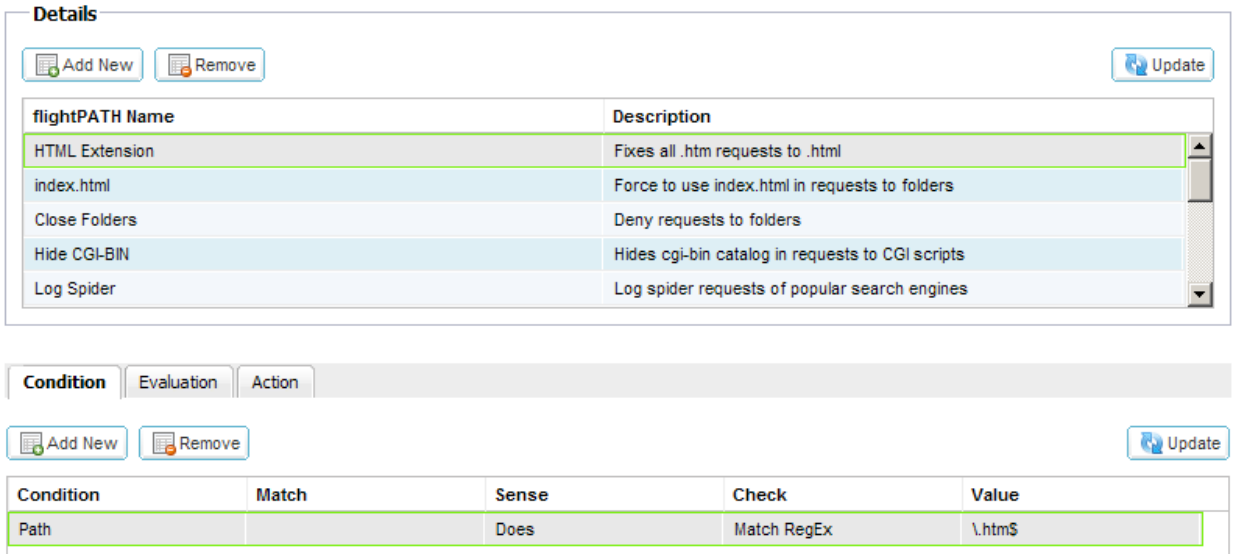
Channel service 10.0.34.100 listening on port 80 I will modify the actions to now use the Health check monitor. Once changed, use the update button to enable this new monitor for the channel service:



You have now configured a new monitor.

flightPATH Menu

Using the Navigation bar on the left of the web interface, go to (Configure →flightPATH) this will open the flightPATH tab allowing you access the flightPATH configuration menus:



The flightPATH screen is broken down into the following sections.

Details

The details screen has a few pre built examples for you to use, and also give you the ability to add new rules.

Conditions

Set multiple criteria to trigger the rule.

Evaluation

Variables that can be used in the Action.

Actions

The behaviour once the rule has triggered.

What is flightPATH?

flightPATH is a rule engine developed by jetNEXUS to intelligently manipulate and route HTTP and HTTPS traffic. It is highly configurable, very powerful and yet very easy to use.

A flightPATH rule has three components:

Conditions
Evaluation
Actions

What can flightPATH Do?

flightPATH can be used to modify Incoming and Outgoing HTTP/S content and requests. As well as using simple string matches such as “Starts with”, “Ends With” etc. For more complete control powerful Perl compatible regular expressions can be implemented.

In addition, custom variables can be created and used in the Action enabling many different possibilities.

Due to the configurable nature of flightPATH the options are infinite but some common uses are as follows.

Application firewalling and Security

- Block unwanted IP’s
- Force user to HTTPs for specific (or all) content
- Block or redirect spiders
- Prevent and alert cross site scripting
- Prevent and alert SQL injection
- Hide internal directory structure
- Rewrite cookies
- Secure directory for particular users

Features

- Redirect users based on path
- Provide Single sign on across multiple system
- Segment users bases on User ID or Cookie
- Add headers for SSL offload
- Language detection
- Rewrite user request
- Fix broken URL’s
- Prevent directory access/ browsing
- Send spiders different content

How do I build a flightPATH rule?

A flight path rule consists of conditions and actions. Multiple conditions can be added and are always added together.

To add a new rule click the Add New button on Details, this enables you to give the flightPATH rule a name and also a Description:

Multiple actions can also be created and are all executed if the conditions are met. Variables can also be created to set values to be dynamically included on the action response.

flightPATH is preloaded with example rules for you to use these are listed below with the definitions.

Pre-Built rules:

HTML Extension

Fixes all .htm requests to .html.

Index.html

Force to use index.html in requests to folders.

Close Folders

Deny requests to folders.

Hide GCI-BIN

Hides cgi-bin catalogue in requests to CGI scripts.

Log Spider

Log spider requests of popular search engines.

Force HTTPS

Force to use HTTPS for certain directory.

Media Stream

Redirects Flash Media Stream to appropriate channel.

Swap HTTP to HTTPS

Change any hardcoded HTTP:// to HTTPs://

Black out credit Cards

Check that there are no credit cards in the response and if one is found, blank it out.

"Content Expiry"

Add a sensible content expiry date to the page to reduce the number of requests and 304s.

Spoof Server Type

Get the Server type and change it to something else.

Never send errors

Client never gets any errors from your site.

Redirect on language

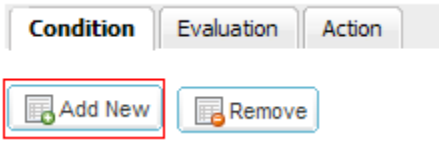
Find the language code and redirect to the related country domain.

Google analytics

Insert the code required by Google for the analytics - Please change the value MYGOOGLECODE to you Google UA ID.

Conditions

New conditions can be added by clicking, "Add New" button:



Multiple conditions can be used but all must be met for the rule to execute. To use an OR you would need to create an additional flightPATH rule.
Each condition contains three elements and a value or not depending on the condition.
Some conditions can accept two values such as Cookie that can have the Match Value i.e. the cookie name and the Value i.e. the Value of the cookie.

The conditions are listed below:

Condition	Description	Example
Host	This is the host extracted from the URL	www.mywebsite.com or 192.168.1.1
Language	This is the Language extracted from the language HTTP header	This condition will produce a dropdown with a list of Languages
Path	This is the path of the website	/mywebsite/index.asp
Cookie	The is the name of a cookie	
Query	This is the name and Value of a Query as such it can either accept the query name or a value also.	"Best=jetNEXUS" Where the Match is Best and the Value is jetNEXUS
Query String	The whole query string after the ? char	Best=jetNEXUS&Name=Me

Method	This is a drop down of HTTP methods	This is a dropdown that includes GET, POST etc
Version	This is the HTTP version	HTTP/1.0 OR HTTP/1.1
Header	This can be any HTTP Header	Referrer, User-Agent, From, Date
POST	POST request method	Check data being uploaded to a website
<form>		
Response Body	A user defined string in the response body	
Response Code	The http code for the response	200 OK, 304 Not Modified

Sense

The sense allows you to create a positive match or a negative match:

Does	Value is true
Does not	Value is not true

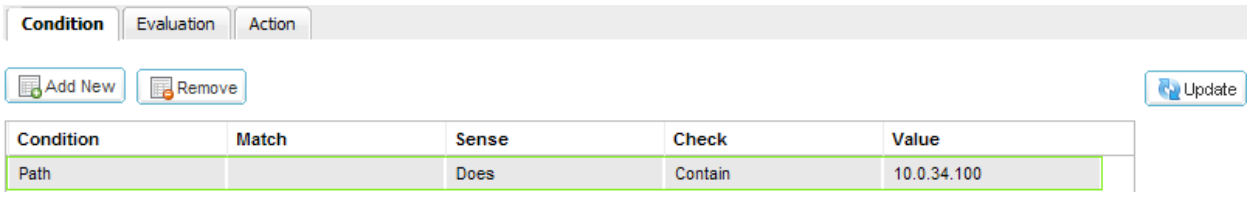
Check

This sets the condition for the rule being fired:

Check	Description	Example
Exist	Check that the Match Item is present	
Start	Check that the Match starts with the value in specified in the Value column	Check Host starts with www Value = www www.jetNEXUS.com = TRUE jetNEXUS.com = False
End	Check that the Match Ends with the value in specified in the Value column	Check Host Ends with com Value = com www.jetNEXUS.com = TRUE www.jetNEXUS.co.uk = False
Contain	Checks any part of the Match for the Value	Check Host Contains jetNEXUS

		Value = jetNEXUS www.jetNEXUS.com = TRUE www.jetNEXUS.co.uk = TRUE www.mywebsite.com = FALSE
Equal	Check the Mach for an exact match	Check Host Equals jetNEXUS Value = jetNEXUS www.jetNEXUS.com = FALSE jetNEXUS = TRUE
Have Length	Check the length of the match	Check the length of the Host Value=16 www.jetNEXUS.com = TRUE www.jetNEXUS.co.uk = FALUE
Match RegEX	This enables you to enter a full Perl compatible regular expression.	**Test for IP Address** ^(25[0-5]|2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9])\.(25[0-5]|2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9]|0)\.(25[0-5]|2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9]|0)\.(25[0-5]|2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[0-9])$

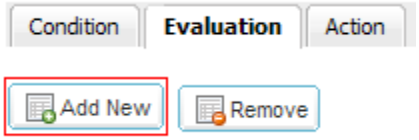
Example: We can create the Condition if the Path does contain the IP Address 10.0.34.100, the Actions and Evaluations can be applied to it:



Evaluation

Adding a Variable is a very powerful feature that will allow you to extract data from the request and include this in the actions. For example you could log a user username or send an email if there is a security problem.

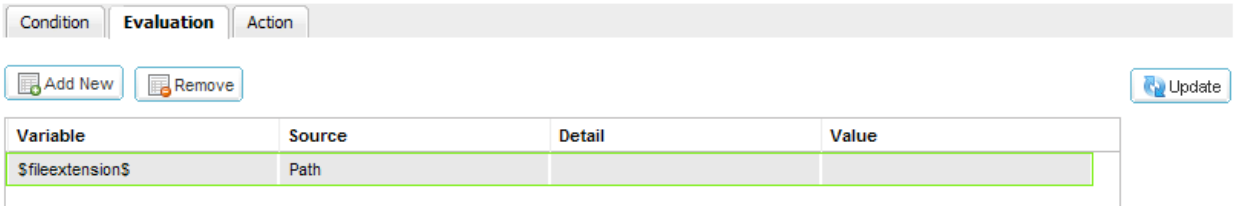
New Variables can be added by clicking, “Add New” button:



A variable name has to be in the following format $name$

So for example we would like to create a variable of the file extension

$fileext$ = Path (From the drop down) = (.*\.)+(.+)



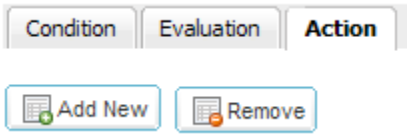
Source

Condition	Description	Example
Host	This is the host extracted from the URL	www.mywebsite.com or 192.168.1.1
Language	This is the Language extracted from the language HTTP header	This condition will produce a dropdown with a list of Languages
Path	This is the path of the website	/mywebsite/index.asp
Cookie	The is the name of a cookie	
Query	This is the name and Value of a Query as such it can either accept the query name or a value also.	“Best=jetNEXUS” Where the Match is Best and the Value is jetNEXUS
Query String	The whole query string after the ? char	Best=jetNEXUS&Name=Me
Method	This is a drop down of HTTP methods	This is a dropdown that includes GET, POST etc

Version	This is the HTTP version	HTTP/1.0 OR HTTP/1.1
Header	This can be any HTTP Header	Referrer, User-Agent, From, Date
POST	POST request method	Check data being uploaded to a website

Actions

New actions can be added by clicking, "Add New" button:

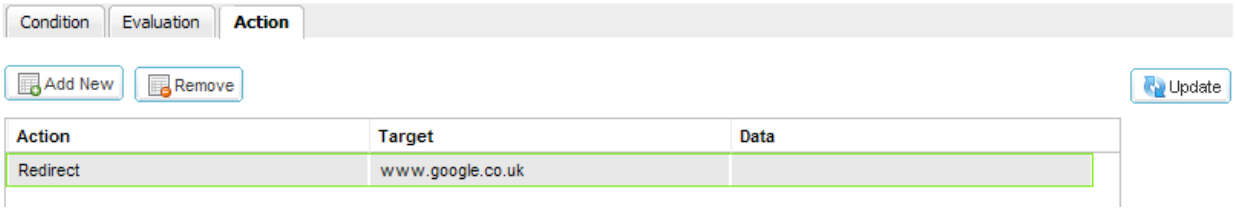


The action is the task or tasks that are enabled once the rule is fired. All actions are fired:

Actions	Description	Data
Rewrite Path	This will allow you to redirect the request to new URL	
Redirect	This will issue a permanent redirect	You can use this redirect to HTTP:// by setting a Variable to the path and URL
Log Event	This will log an event to the System log	
e-Mail	Will send an email. You can use a variable as the address or the message	
Drop	This will drop the connection	
Use Server	Select which server to use	Content server
Body Replace First	Body replacement first	Replace with
Body Replace Last	Body replacement last	Replace with
Body Replace All	Body replacement All	Replace with
Replace Request Header	Replace request header	Replace header information
Add Request Header	Add request header	Add new header information
Replace Response Header	Replace the response header	Replace header information
Remove Response Header	Remove the response header	Remove header information

Add Response Header	Add request header	Add new header information
Replace Request Cookie	Replace request cookie	Add new cookie
Remove Request Cookie	Remove request cookie	
Add Request cookie	Add request cookie	Add new cookie

Example: We can create a redirect action so the URL is redirected to an external site:



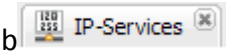
Target

Target	Description	Data
From	The email address of the user making the request	From: user@example.com
Accept	Content-Types that are acceptable	Accept: text/plain
Accept-Encoding	Acceptable encodings	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Acceptable languages for response	Accept-Language: en-US
User-Agent	The user agent string of the user agent	User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Referer	This is the address of the previous web page from which a link to the currently requested page was followed	Referer: http://www.jetnexus.com
Cookie	an HTTP cookie previously sent by the server with Set-Cookie (below)	Cookie: $Version=1; Skin=new;
Set-Cookie	an HTTP cookie	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Authorisation	Authentication credentials for HTTP authentication	Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Contains account information for the costs of the application of the method requested	

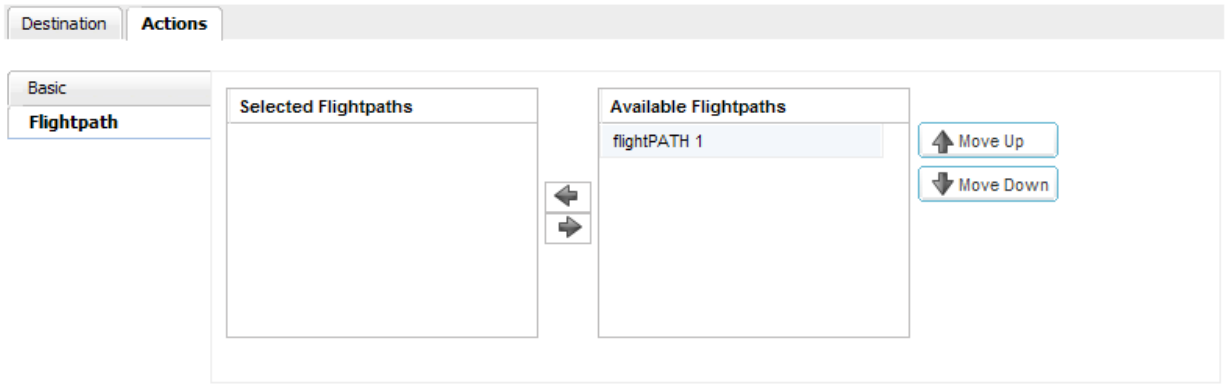
If-Modified-Since	Allows a *304 Not Modified* to be returned if content is unchanged	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Pragma	Implementation-specific headers that may have various effects anywhere along the request-response chain.	Pragma: no-cache
Content-Type	The mime type of the body of the request (used with POST and PUT requests)	Content-Type: application/x-www-form-urlencoded
Content-Encoding	The type of encoding used on the data. See HTTP compression	Content-Encoding: gzip
Last-Modified	The last modified date for the requested object, in RFC 2822 format	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Accept-Ranges	What partial content range types this server supports	Accept-Ranges: bytes

How do I apply flightPATH rules?

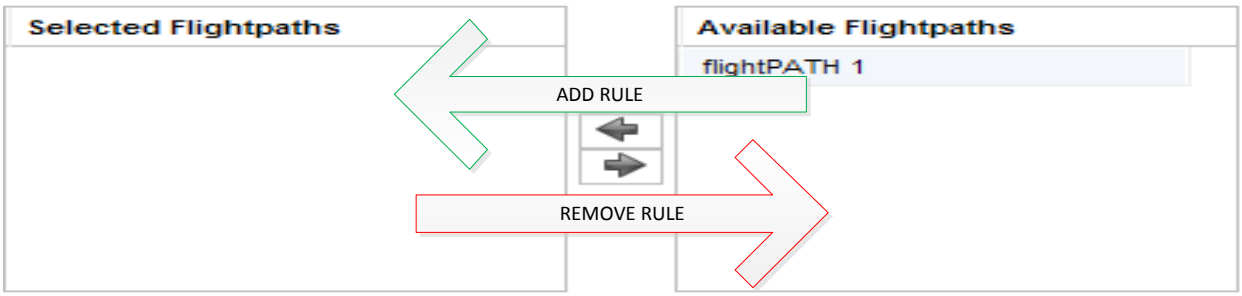
flightPATH rules are designed to manipulate HTTP traffic as such the option for flightPATH is not visible for non HTTP protocols.

To enable a flightPATH rule go to (Setup →IP Services*)* page. This will open the IP Service tab 

flightPATH rules can be applied in the IP services screen under Action:

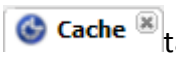


The list of available rules is on the right and the current rules in use are on the left. To add a new rule drag and drop the rule into position:



The order for execution is important and will start with the top rule being executed fist. To change the order simple drag and drop into the correct location. To remove a rule simply drag and drop it back to the rule inventory.

Caching

Using the Navigation bar on the left of the web interface go to (Configure →Cache). This will open the 

tab allowing you to access the caching configuration screen.

How jetNEXUS Caching Works

Upon receipt of a request, the cache is searched for the requested page. The request is forwarded to a local content server group if the page cannot be found in the cache.

If it is in cache, but expired, a revalidation request is used with the most recent "If-Modified-Since" value. If the cache entry is OK (i.e. if the content matches "If-Modified-Since") a cache local "304 Not Modified" is returned, otherwise a cache local "full response" is sent.

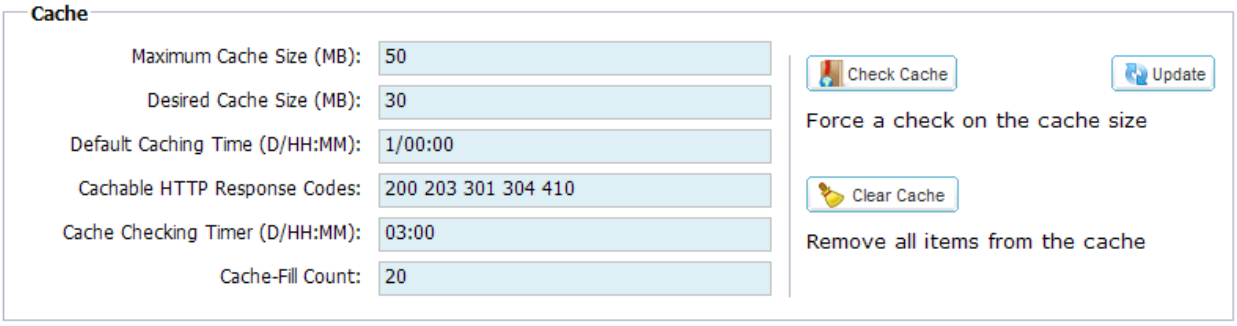
Note that the cache stores only uncompressed content as page acceleration is performed after the page is taken from the cache.

Upon filling the cache, the oldest (least recently used) content is retired from cache in order to make room for the new content. When the cache size meets the maximum size, or when the timer triggers a check, or when the "check cache" button is clicked, a cache check is performed.

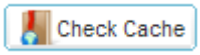
Whilst the size of the cache is greater than the desired, content is removed from the cache as described above. Once the desired size is reached, the cache is left to grow naturally until the next check is triggered.

The Caching screen is divided into three parts:

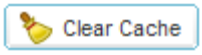
Parameters to configure overall cache behaviour



Note.

The 

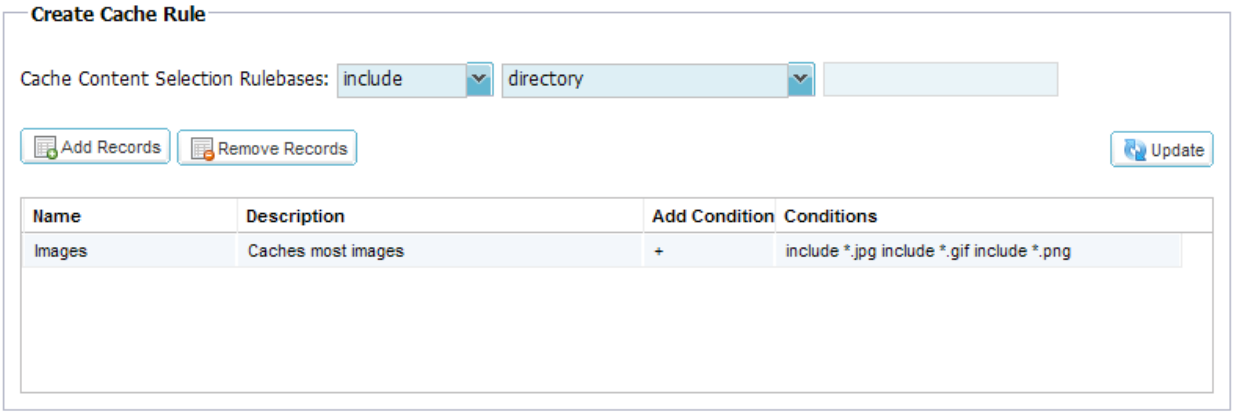
button, clears the cache of expired items no longer being served:

The 

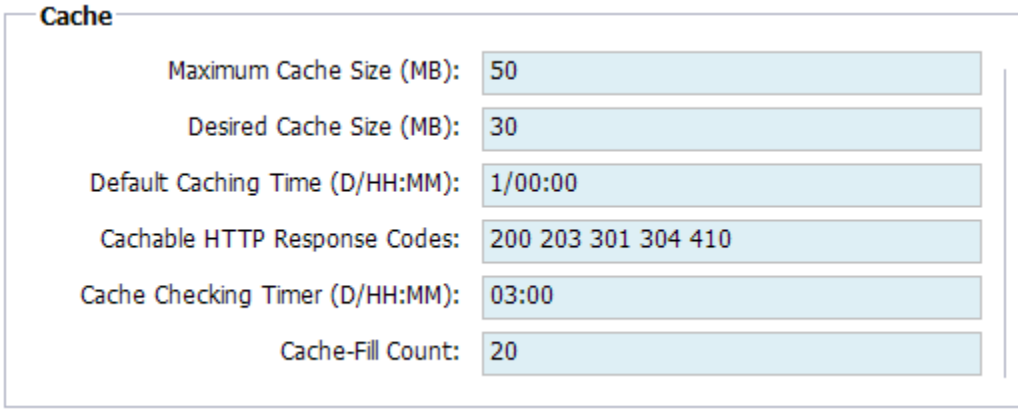
button, clears the cache of all content.

Parameters to defined Rule Bases to domains

Parameters to define one or more caching Rule Bases



Cache Settings



The parameters related to overall caching behaviour are as follows:

Maximum Cache Size (MB): Maximum RAM that the cache can consume.

The jetNEXUS Cache is an in-memory cache that is also periodically backed onto hard disk to maintain cache persistence after restarts, reboots and shutdowns. This means that the maximum cache size must fit within the memory footprint of the appliance (rather than disk space) and should be no more than half of available memory.

Recent jetNEXUS ALBs are equipped with 2GB of RAM while older models are fitted with 1GB. For 1GB of RAM the cache size should be no more than 512MB, while appliances with 2GB of RAM should have a cache size no larger than 1GB. Increasing the cache size beyond this limit could adversely affect page acceleration if the compressed content is large, so care must be exercised.

Calculating the best cache size for your site(s) will obviously depend on the amount of cacheable content you have, but you may find it equally effective to start with the default cache size (50MB). A periodic review of the stats for caching under “Monitor -> Statistics” (where the cache contents are described in terms of bytes used and percentage filled) will then help you decide whether to reduce or expand the maximum cache size. Be aware that this value is also complemented by a desired cache size (see below).

Desired Cache Size (MB): Optimum RAM that the cache will be trimmed to.

While the maximum cache size represents the absolute upper boundary of the cache, the desired cache size is intended as the optimum size that the cache should attempt to attain whenever an automatic or manual check on the cache size is made.

The gap between the maximum and desired cache size exists to accommodate the arrival and overlap of new content between periodic checks on cache size for the purpose of trimming expired content. Once again, it may be more effective to accept the default value (30 MB) and periodically review the size of the cache under “Monitor -> Statistics” for appropriate sizing.

Setting the desired and maximum cache sizes to the same figure will cause the cache to be trimmed with every request fetching new content into the cache. There are conditions where this may be desirable, but there will also be an impact on performance in that cache content is being shuffled in and out of the cache continuously.

Default Caching Time (D/HH:MM): Life of content without an explicit expiry value.

The default caching time is the period content will be stored in the cache for items that don’t have a “no-store” directive, but also have no explicit expiry time in the traffic header. The field entry takes the form “D/HH:MM” - so an entry of “1/00:00” (the default) means to store the item for one day, “01:00” for one hour and “00:01” for one minute.

Cacheable HTTP Response Codes: HTTP responses that will be cached.

This field should be edited with caution as the most common cacheable response codes are already listed:

200 - Standard response for successful HTTP requests.
203 - Headers are not definitive, but are gathered from a local or a 3rd party copy.
301 - The requested resource has been assigned a new permanent URL.

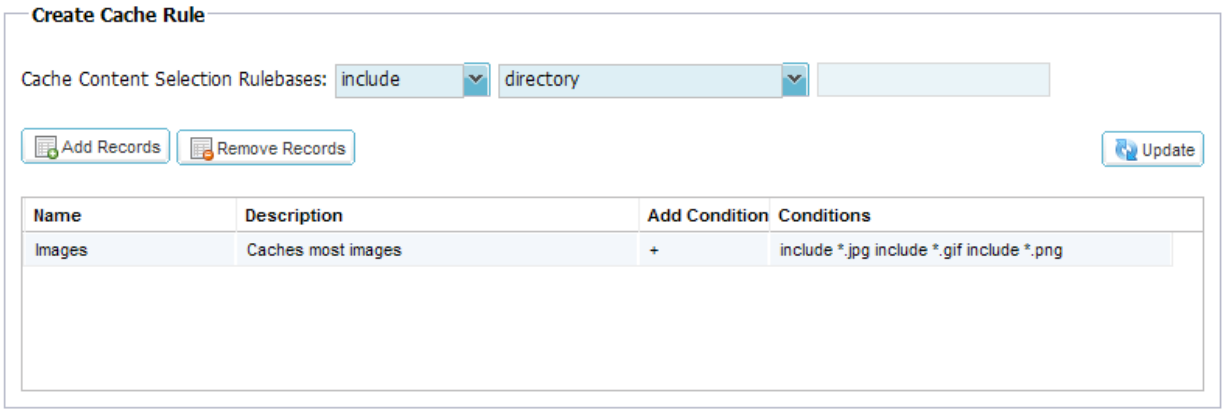
304 - Not modified since the last request, and the locally cached copy should be used instead.
410 - Resource is no longer available at the server and no forwarding address is known.

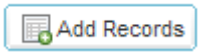
Cache Checking Timer (D/HH:MM): Interval between cache trim operation

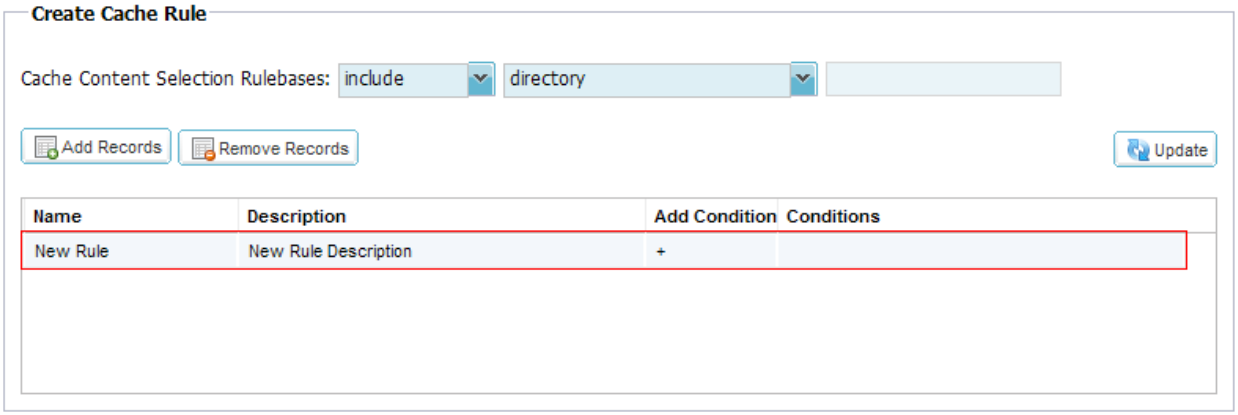
Cache-Fill Count: Count of 304s for a cached item before re-fetching

Adding a Caching Rule

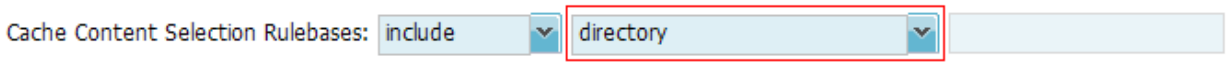
The (Configure →Cache) screen also supports the creation of custom rule bases that can later be applied against one or more domain names being managed by the cache (more on this in the last part of this section):



Press the  button to add a rule base and series of fields are displayed:



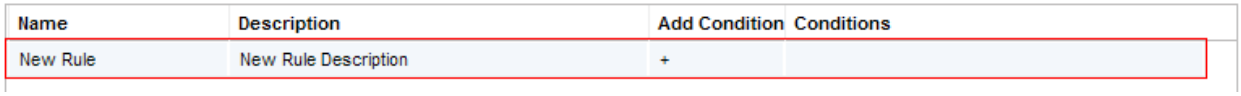
Most caching rules can be added using the menu below, the options are explained below:



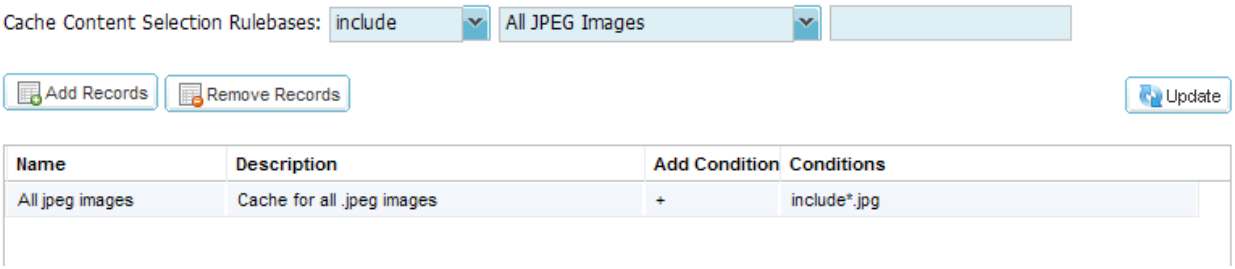
Directory:	Anything in the named directory anywhere on the site
File:	Any file so named please include any file extension
Anything starting:	The prefix to the URL (including the leading / character)
Anything ending:	The suffix to the URL (including file name or trailing /)
Anything containing:	A significant piece of the URL anywhere within it
Exact match:	The exact URL of a piece of content

All JPEG Images:
All GIF Images:
All Bitmap Images:
All PNG Images:
All HTML Pages:

Name:	Short name of the rule base
Description:	Informative description of the rule base.
Add Condition:	+ to add rule
Conditions:	Added by Cache content selection



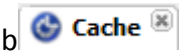
Most rules are "include" rules, but you can subsequently "exclude" subsets of content if required. Leave "include" selected for the first rule:

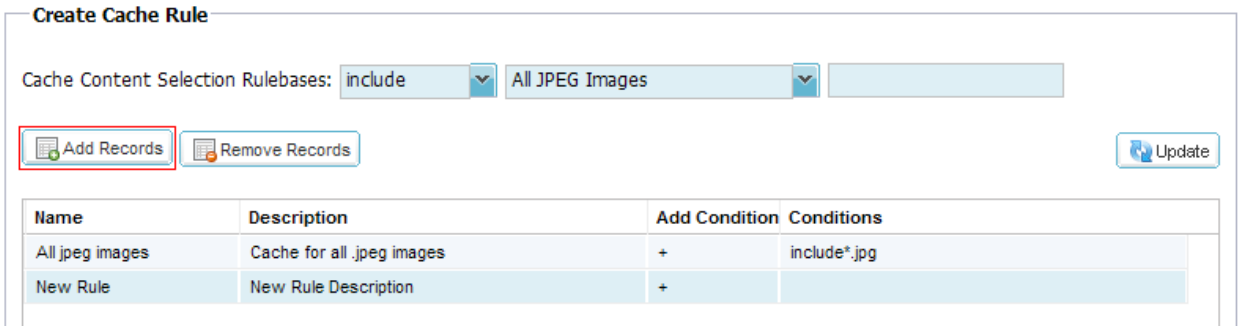


Then select the type of content you'd like to include in caching, in the example above we have decided to cache all *.jpg images.

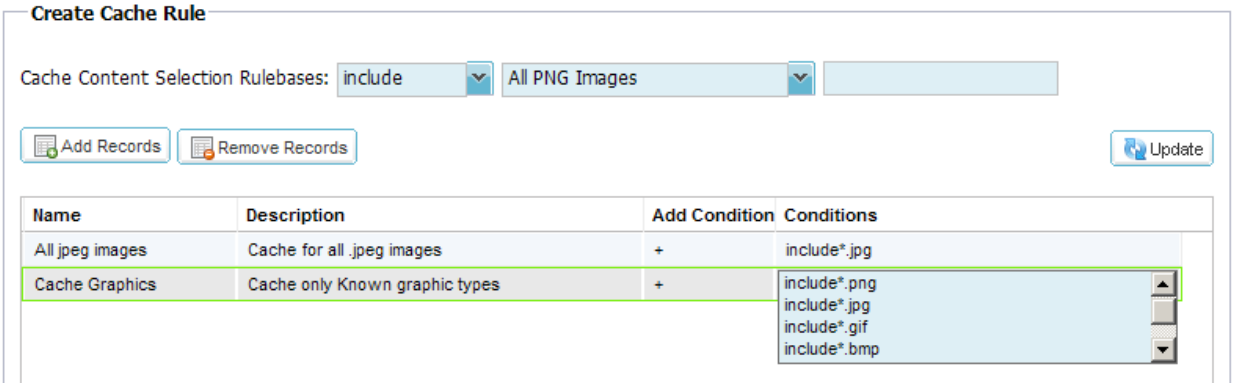
The Add condition + will add whatever content you have selected in the Cache Content Selection Rulebase screen and update the conditions section for you.

Creating a Caching Rule

To Set up Caching you will need to access the settings in the following location (Configure →Cache). This will open the Caching tab 



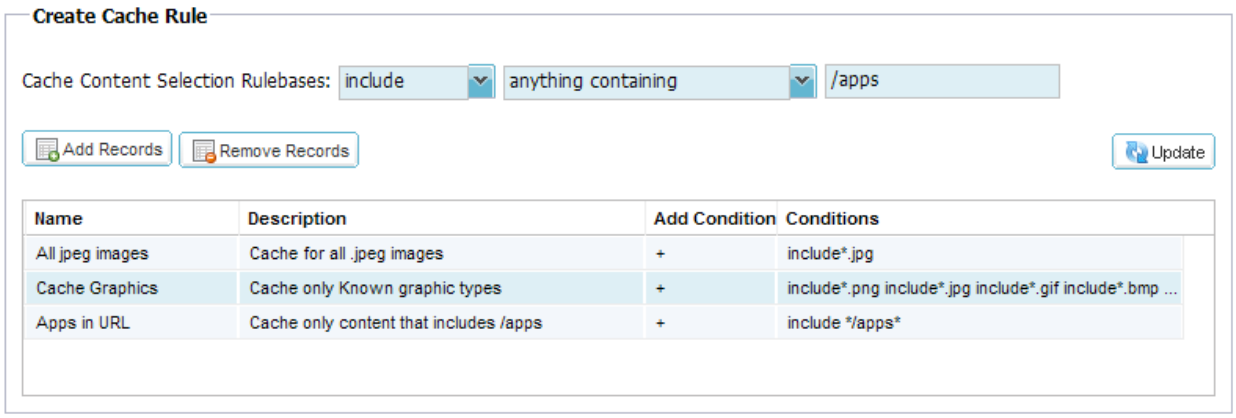
Our first example rule will be called “Cache Graphics” and will restrict content to the known graphic types already shown in the dropdown list (see below):



Pressing the 

will add the “Cache Graphics” rulebase.

Our next example rule will be called “apps in URL” and will restrict caching to content whose text contains “/apps/” anywhere in the URL:



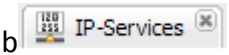
If there's a mistake in any of the values, you can either edit or delete the line later. Click the 

button to make the changes take effect.

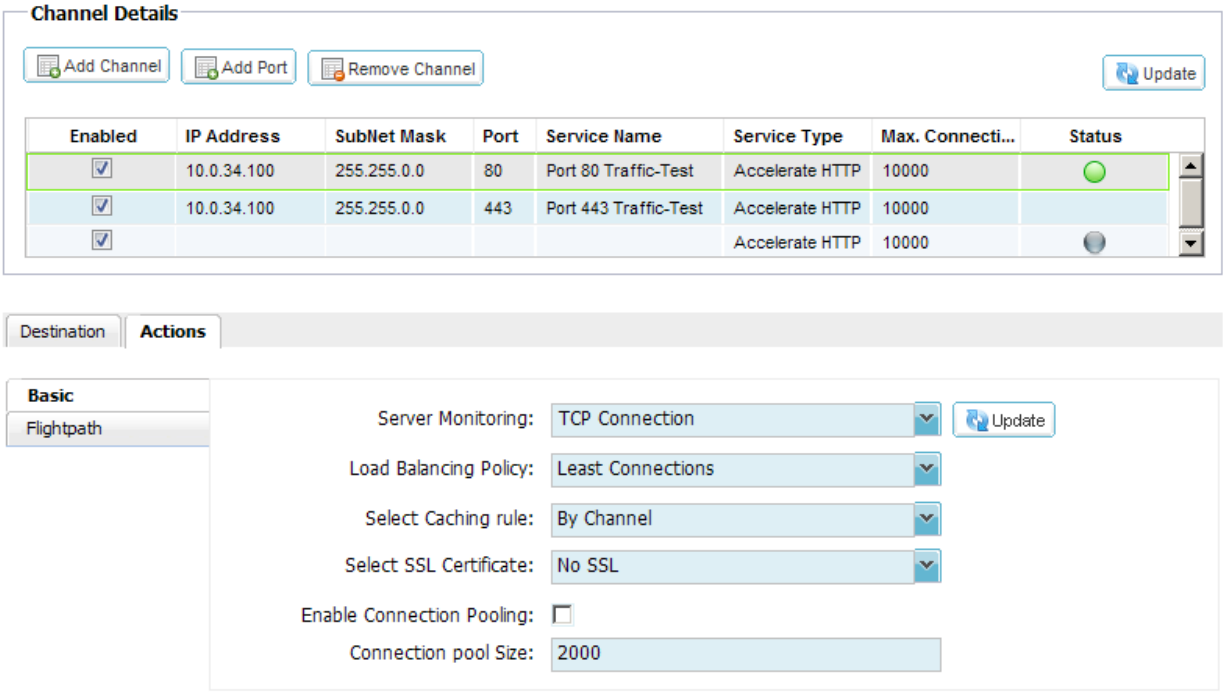
Remember that you can edit the content and click the 

button again at any time to revise the rule base.

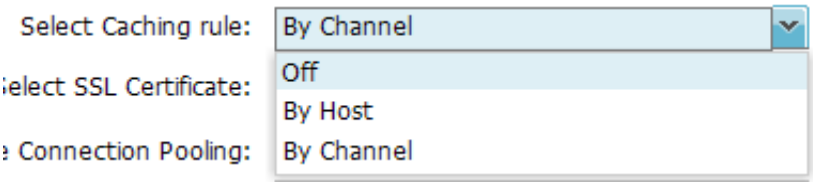
Associating Domains to a Cache Rule base

You will need to first Activate the caching checkbox in (Setup →IP Services*)*. This will open the IP Service tab 

Select the channel you wish to enable caching on, and click on the actions tab:



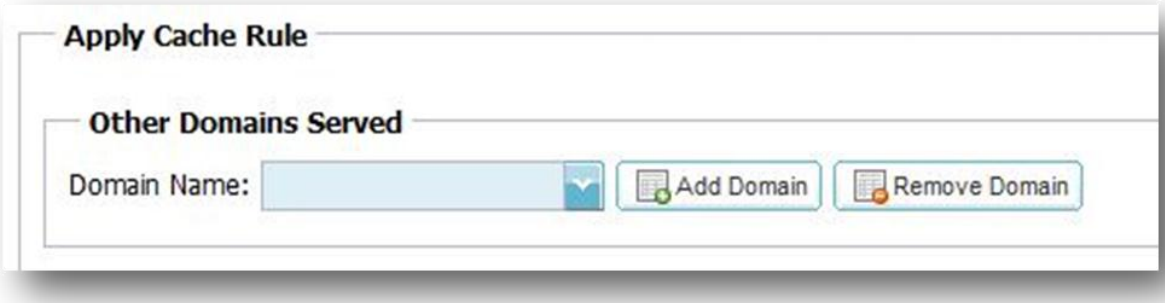
You are then given 3 options:



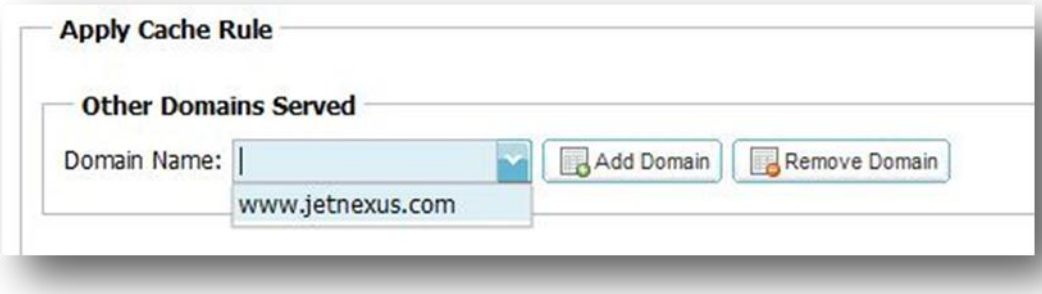
By Host

Once “By host” is enabled the ALB will then begin monitoring the domain names served to clients via the defined Channel.

Prior to activation, the middle section of the (Configure →Cache) screen was empty:



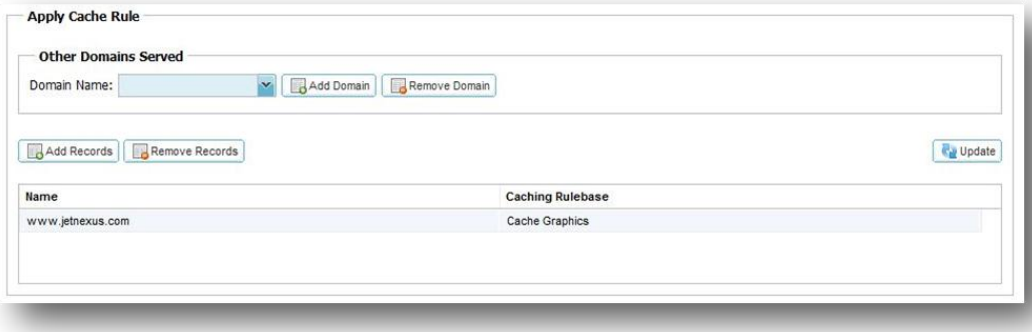
With caching activated and traffic passing through the ALBX, any domains served (though not yet cached) via the Channel will appear in the middle section (in our example www.jetnexus.com):

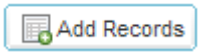


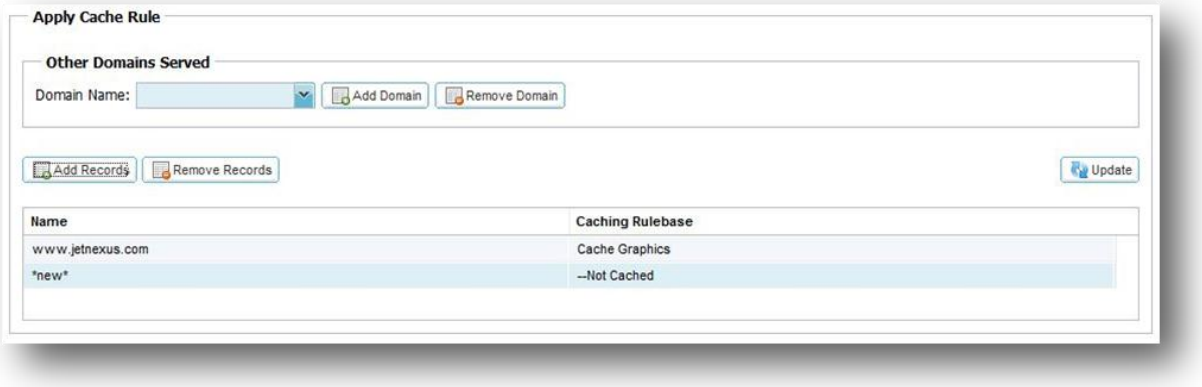
By pressing the "<-"arrow next to the domain name "www.jetNEXUS.com", the domain is added to the cached domains list and a caching rulebase can be applied:

Note that the dropdown list of available rulebases includes the two examples we defined earlier in this section.

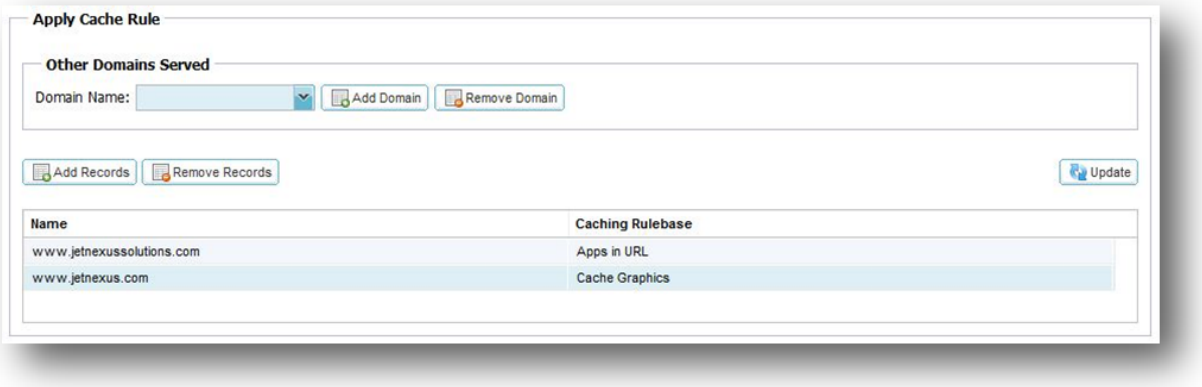
Select one of the rulebases in the list and press the  button at the right of this section to apply the change:



Domain names can also be added manually (rather than waiting for the ALBX to collect them for you) by pressing the  button:



Enter the domain name you want to add, select a caching rulebase from the dropdown list and press the "[Update]" button:



This completes the activation and configuration of ALBX by host caching.

By Channel

Prior to activation, the middle section of the (Configure →Cache) screen was empty.

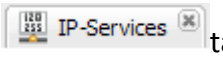
Once By Channel is enabled the ALB will then begin monitoring the Listening IP and port: (Example: 10.0.34.100:80)

You can monitor caching behaviour via the (Monitor →Cache) screen:

Content Statistics

You have now configured a Caching

Connection Pooling

Using the Navigation bar on the left of the web interface, go to (Setup →IP Services*)* page. This will open the 

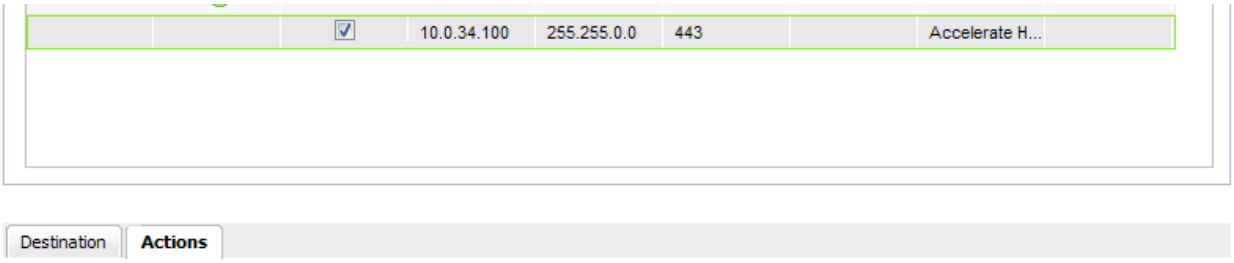
tab.

What is connection pooling?

Connection pooling minimises the connections to the content servers, recycling these connections as fast as possible to service client requests.

Enable connection pooling?

To access the pooling, select the Channel IP you wish to modify and click on actions:



Tick the Enable connection pooling box, and enter the pool size which is normally set to 2000 or less:

Once the simultaneous requests on each server reach the pool size, the connections are capped. Additional client requests will use the next free connection. The content servers will service requests quickly leaving ALB to maintain scalability on the client-side.

You have now configured connection pooling

SSL Offload and termination

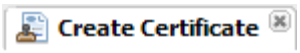
What can jetNEXUS do with SSL?

jetNEXUS ALB has the ability to offload the SSL encryption and decryption work load from your backend servers and also becoming the termination point for your SSL certificates. jetNEXUS also has the ability to re-encrypt traffic to the back-end content servers for more secure environments.

SSL Tasks that can be completed on the jetNEXUS ALB

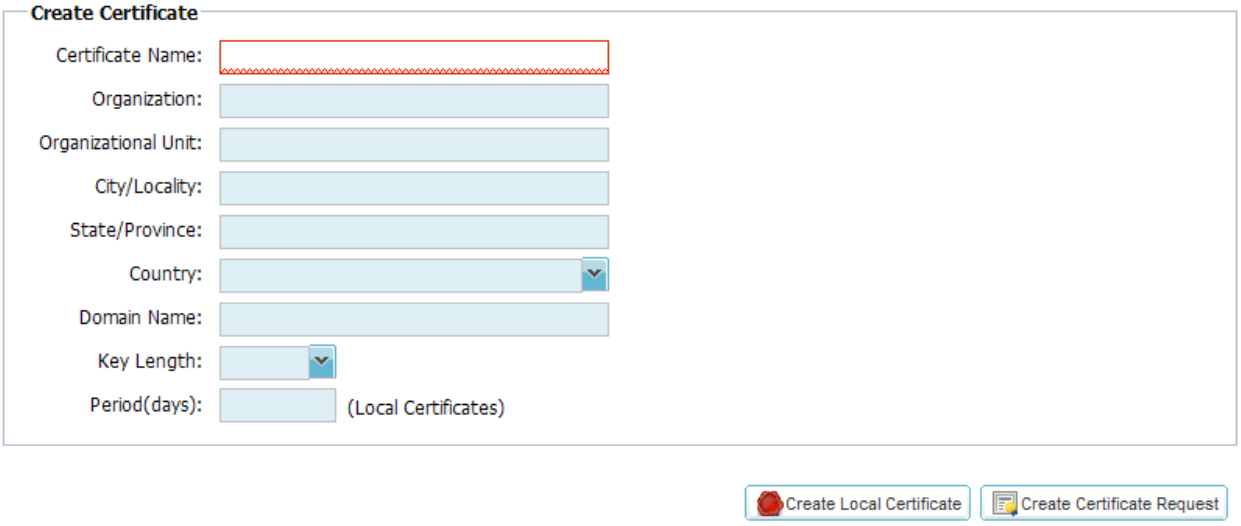
- Create Self Signed Certificates
- Create Certificate Requests for Certificate Authorities
- Install Trusted Certificates supplied by a Certificate Authority
- Importing certificate from an IIS server
- Importing certificates from a Apache Web server
- Importing certificates from another jetNEXUS Accelerator
- Export Certificates to be used another jetNEXUS ALB or web Server
- Configure Listening Interfaces as SSL interfaces
- Configure content server for SSL

Creating A Self Signed Certificate

Using the Navigation bar on the left of the web interface, go to (Configure →SSL) Click on 

this will open the create certificate tab.

You will then be presented with the Create Certificate screen:



Each field will need to be filled in a description of each field is detailed below.

Certificate Name

A unique name which will identify the certificate when it is created Avoid use of **£ $ / . * ? < > - &** and all types of quotes.

Organization

Organization information for the certificate.

Organizational Unit

Add the appropriate information for the certificate.

City /Locality

Location information for the certificate.

State/Province

Location information for the certificate.

Country

Location information for the certificate.

Domain Name

Domain name information for the certificate.

Key Length

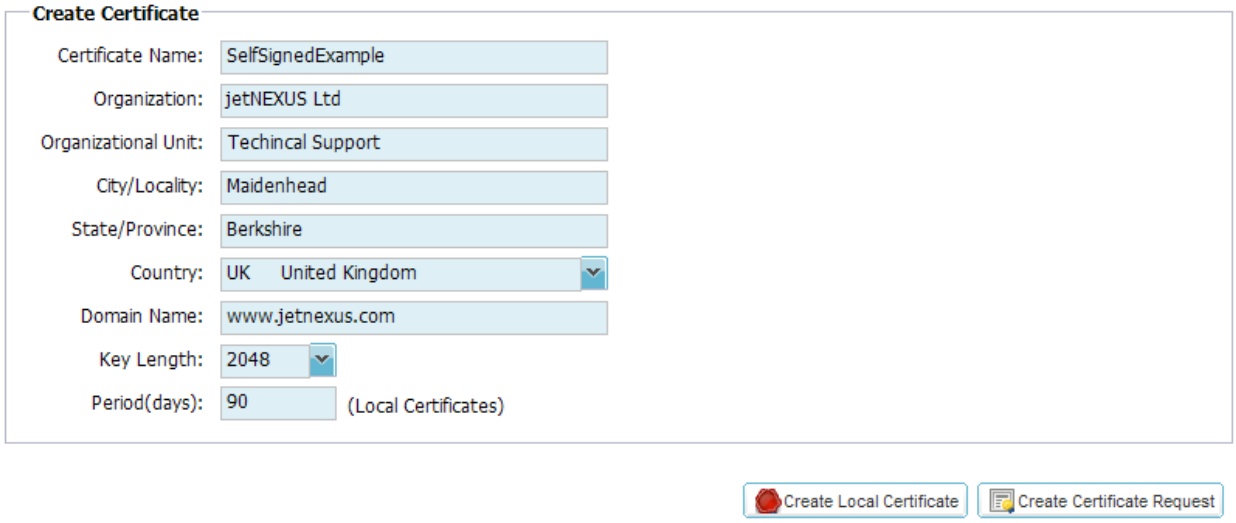
Key Length indicates the length of the RSA key which will be used to generate the certificate.

Period (Days))

Period is only required for Self Signed certificates and indicates the duration of the certificate.

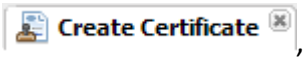
Once the certificate information has been entered, to generate the self-signed certificate, click "*Create Local Certificate*".

A completed self-signed certificate is below.



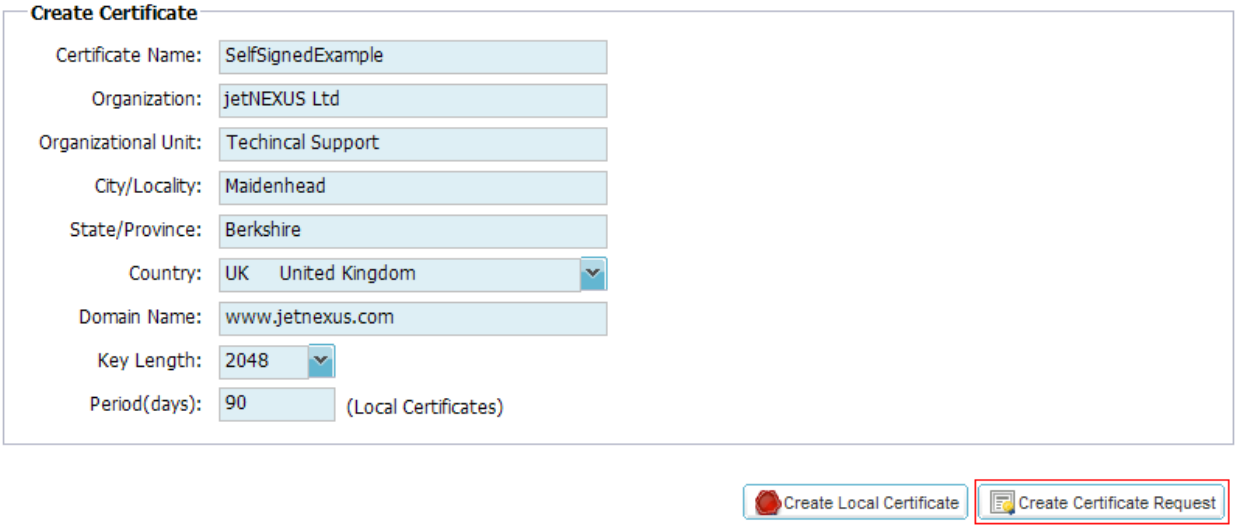
The self-signed certificate is then ready to be assigned to an SSL listening interface.

Creating Certificate Requests

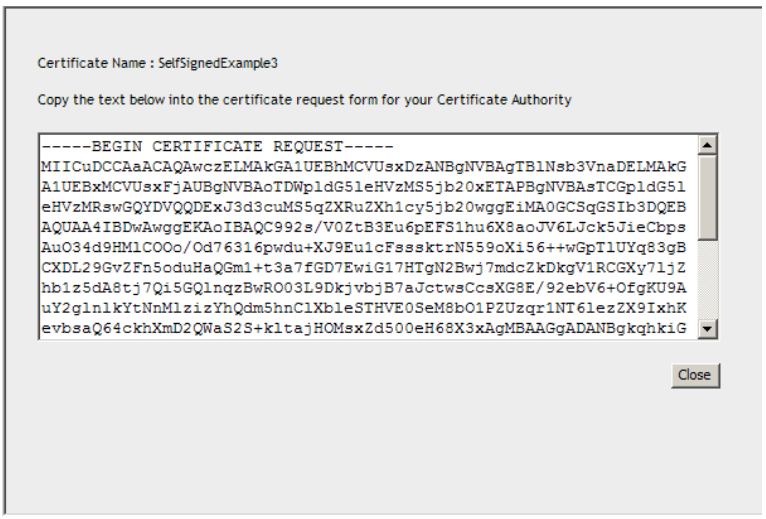
Using the Navigation bar on the left of the web interface, go to (Configure →SSL) Click on 

, this will open the create certificate tab

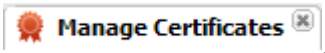
Once the certificate request information has been entered, to generate the certificate request, click "*Create Certificate Request*":



The certificate request is displayed in a popup window, as shown below, so it can be copied into the Certificate Authority Request form:

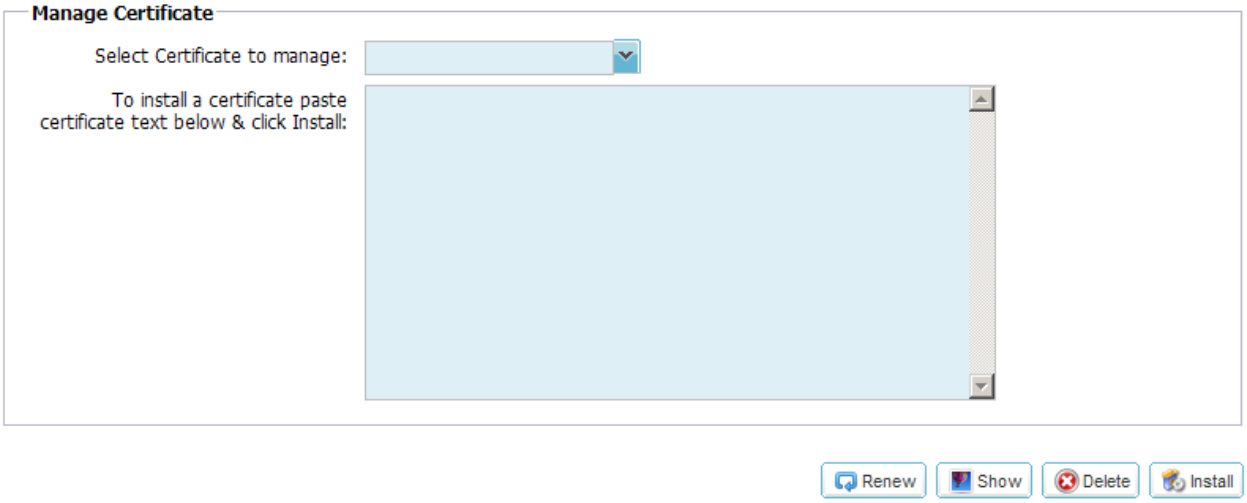


Installing Trusted Certificates

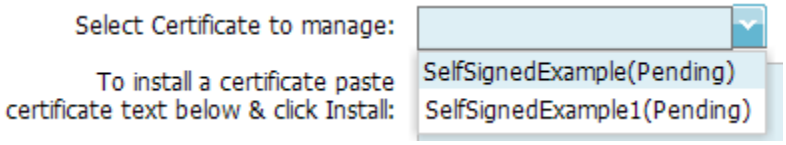
Using the Navigation bar on the left of the web interface, go to (Configure →SSL) (and select 

, This will open the manage certificate tab

Select the corresponding certificate request from the list box on the left hand side of the screen:

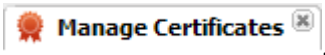


Select the certificate you wish to manage using the drop down:

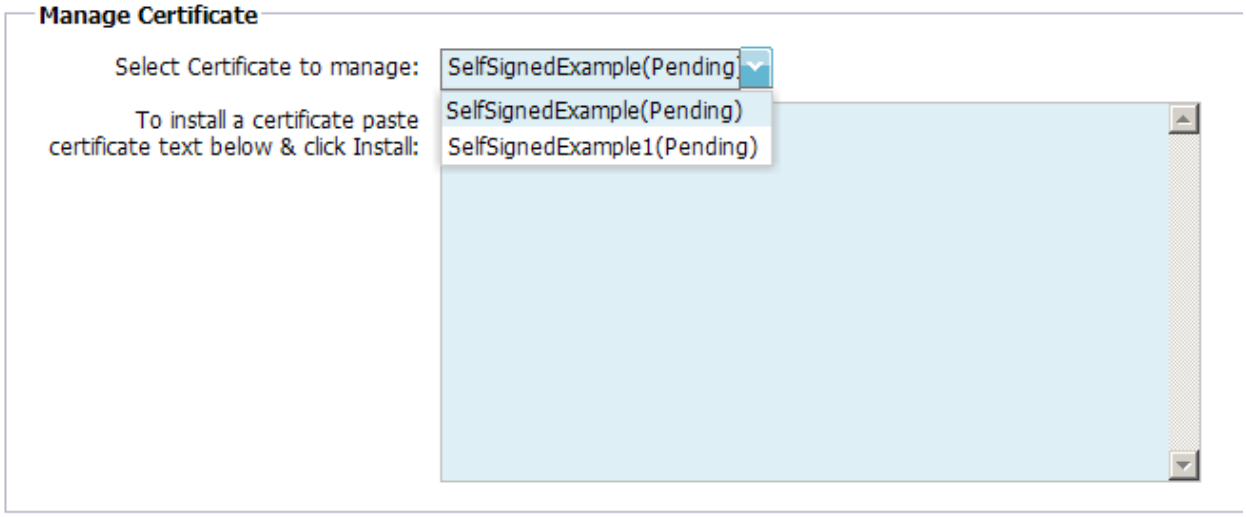


Copy and paste the certificate supplied by the Certificate Authority into the certificate text box on the right hand side of the screen. Finally to install the certificate, click 

Certificate Management

Using the Navigation bar on the left of the web interface, go to (Configure →SSL) and select 

, This will open the manage certificate tab (You can manage your certificates from this screen):



You have 4 options for each certificate:

Renew

The "Renew" button performs the same functions as the "Create Local Certificate" and "Create Certificate Request" buttons on the "Certificate Creation" screen.

If a self-signed certificate has been selected, when the "Renew" button is clicked, the self-signed certificate will be created with the same information supplied on the "Certificate Creation" screen.

If a certificate request or installed trusted certificate is selected the certificate request will be recreated and displayed in a popup window.

Show

The "*Show*" button will display the details of the selected self-signed certificate, pending certificate request or installed trusted certificate in a popup window, as shown below:

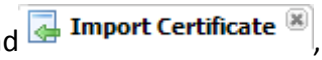
Delete

The *"Delete"* button allows a self-signed certificate, pending certificate request or trusted certificate to be completely removed from the jetNEXUS ALB.

Install

The *"Install"* button allows a certificate to be installed copy and paste the certificate into the field.

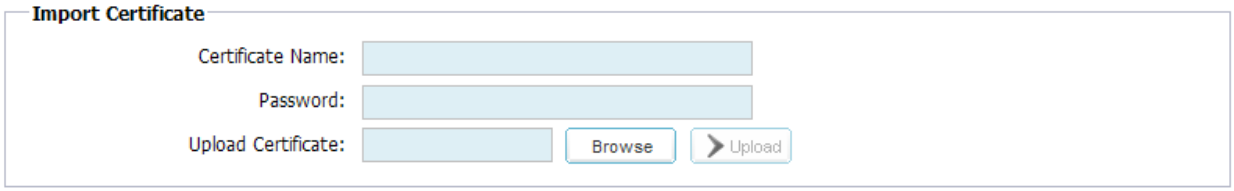
Importing Certificates

Using the Navigation bar on the left of the web interface, go to (Configure →SSL) and 

, this will open the Import certificate tab

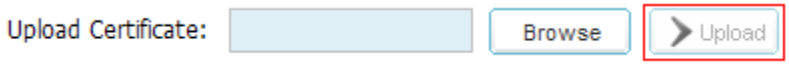
The imported certificate should be a PKCS#12 file and should include an exported private key.

The *Certificate Name* is the name to be used to reference the import certificate. It should be a unique name:

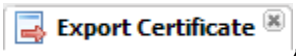


The *Password* is the password supplied when the certificate was exported, either from another jetNEXUS ALB or from an Apache or IIS web Server.

Click browse to locate your certificate, click go to upload it:

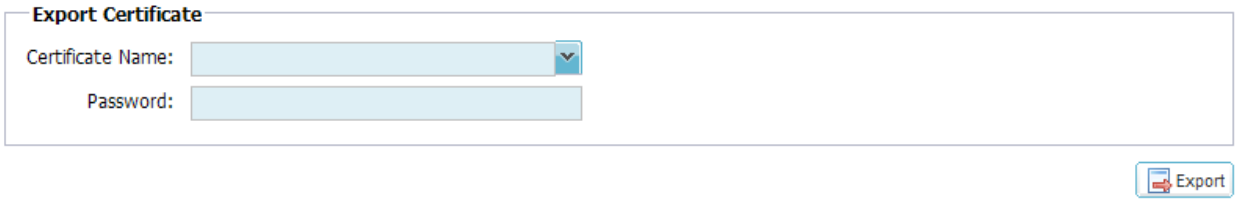


Exporting Certificates

Using the Navigation bar on the left of the web interface, go to (Configure →SSL) and click on 

, This will open the Export certificate tab

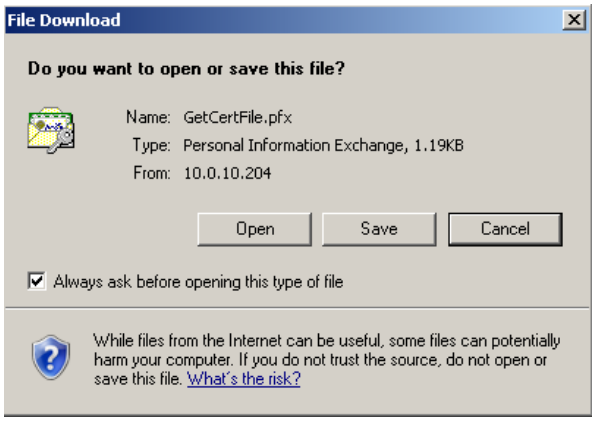
Select the certificate to be exported using the "*Certificate Name*" drop down:



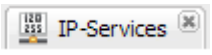
The supplied *Password* will be required when the certificate is imported to another jetNEXUS ALB or to an Apache or IIS web server:

The password must be secure but one you are able to remember, this password should never be sent with the PFX file.

Click Export to export the certificate you will then be asked where to save the file:

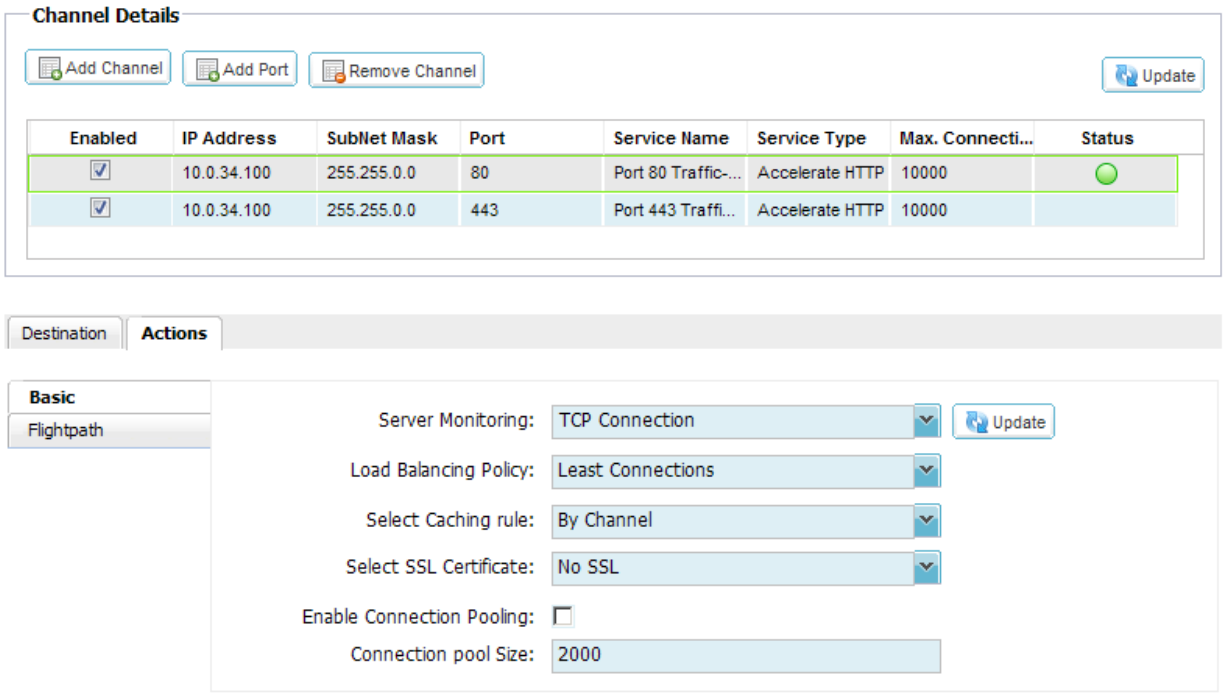


Configuring an SSL Listening Interface

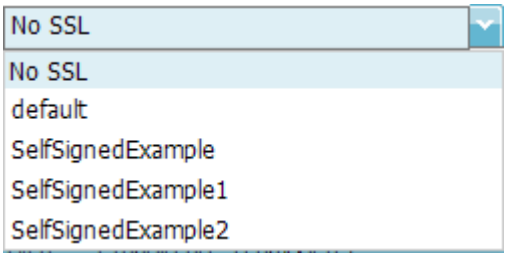
Using the Navigation bar on the left of the web interface, go to (Setup →IP Services) page. This will open the 

tab.

To enable SSL termination, select the Channel IP you wish to enable your SSL certificate on. Then click on the Actions tab:



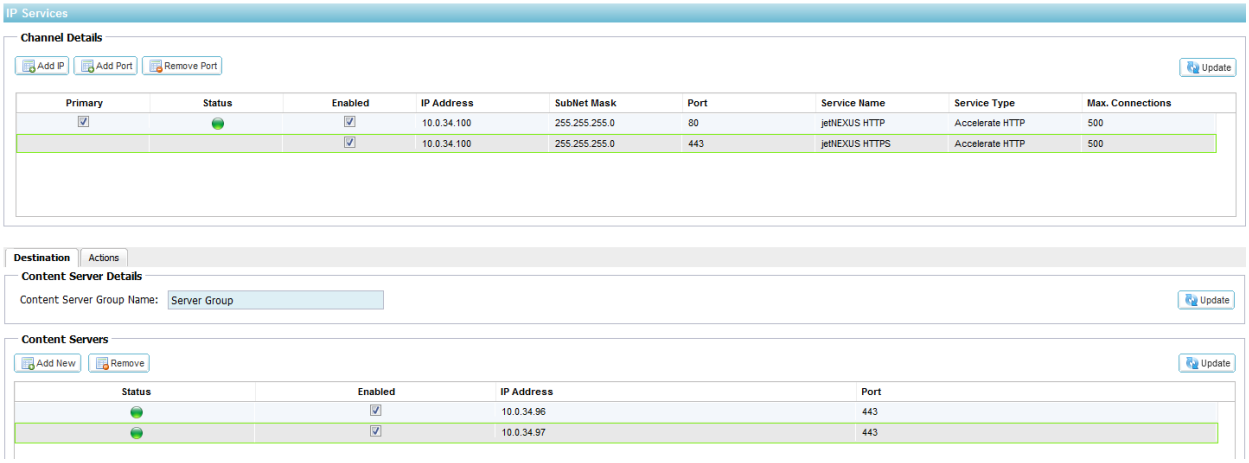
The list of available SSL certificates will include user created self-signed certificates, installed trusted certificates and a default self-signed certificate which is always present on the ALB:



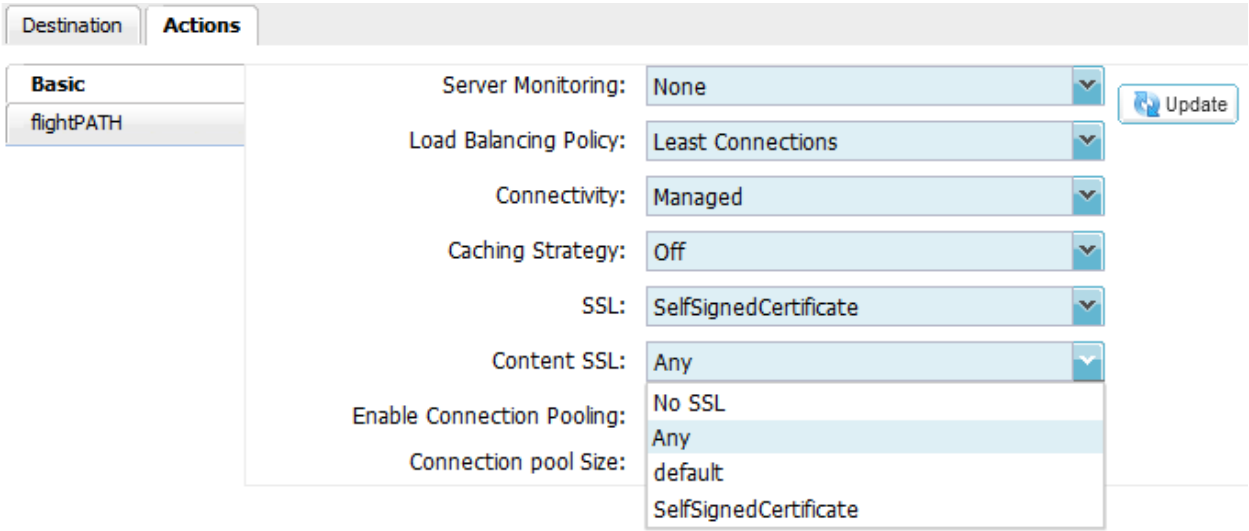
Remember that when SSL offloading the listening port is typically 443 and the web server is not HTTPS i.e. typically HTTP on port 80

Configuring SSL for content servers

This time we configure both the listening port and the content server port for 443

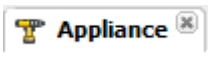


Within the "Actions" tab we must now configure the "Content SSL" section. The drop down box will contain any certificates you have created or imported plus the default certificate installed on the jetNEXUS ALB. Select the "Any" option for the ability accept any content server certificate.



You have now configured a SSL

Failover configuration

Using the Navigation bar on the left of the web interface, go to (Setup →Appliance) page, this will open the 

tab.

For fail over operation, you will need to configure multiple jetNEXUS ALB's with the same listening interface information.

Each additional unit's configuration will need to match, please contact support@jetNEXUS.com if you would like some guidance during this process.

Why use failover?

Failover is used for high availability of your application or web service and also providing hardware redundancy.

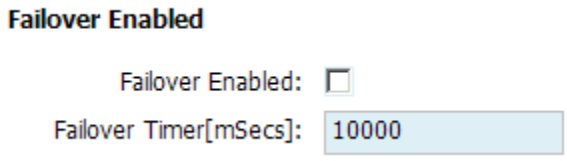
You have 2 main ways to configure jetNEXUS failover

Active/Passive
Using 2 ALB's which work as an Active/Passive cluster where you have 1 unit as Primary serving all connections, and 1 unit as a Secondary/Slave waiting to take the incoming connections if the primary unit fail.

Active/Active
Using 2 ALB's which work as an Active/Active cluster where both units are able to serve different Channel IP's and become the secondary for each service not marked as primary on that unit.

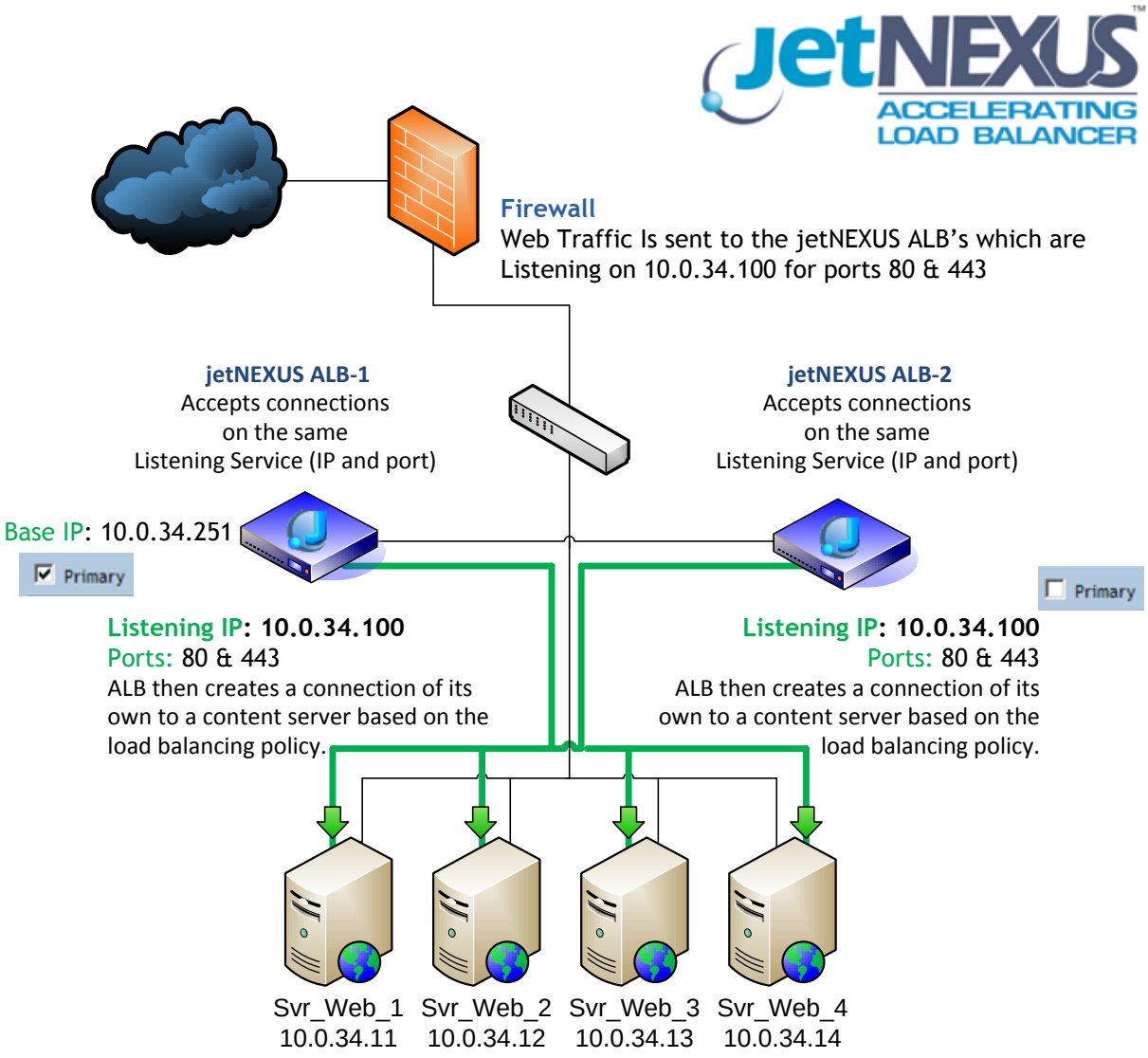
Enabling failover?

You will need to first tick the enable the failover function on the ALB, click update:



Complete this step on each unit you wish to be part of the cluster.

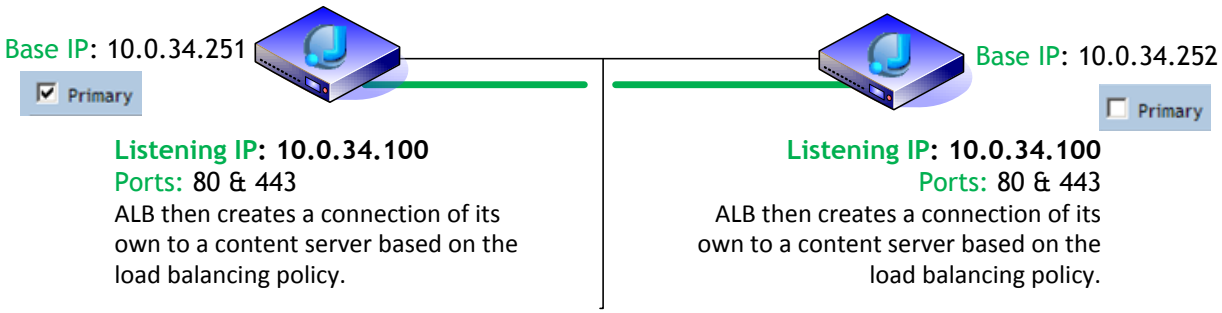
Failover diagram



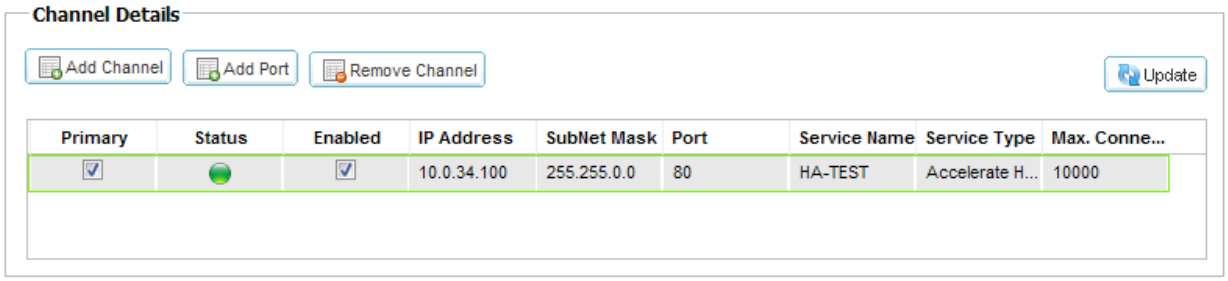
Both units have failover enabled but are using channels to enable failover for services.

Failover diagram explained

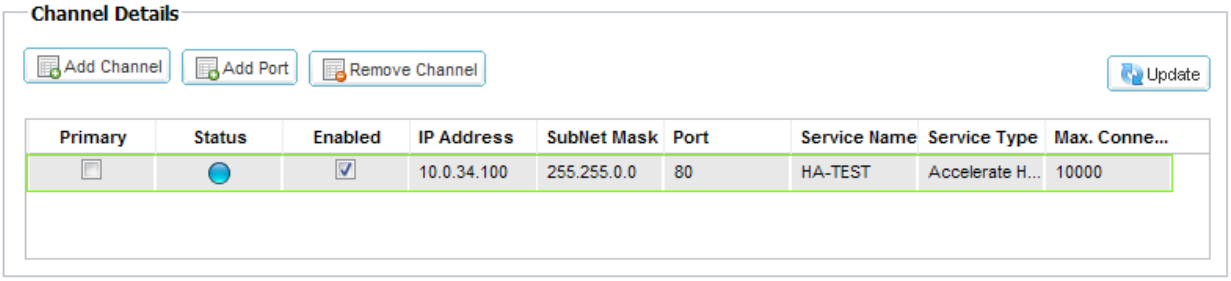
Both units have different Base IP's but the configuration for Channels are the same:



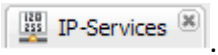
On ALB-1 we have ticked the Primary box on the following channel making this the Primary unit.



On ALB-2 we have not ticked the Primary box on the same channel making this unit the Failover:

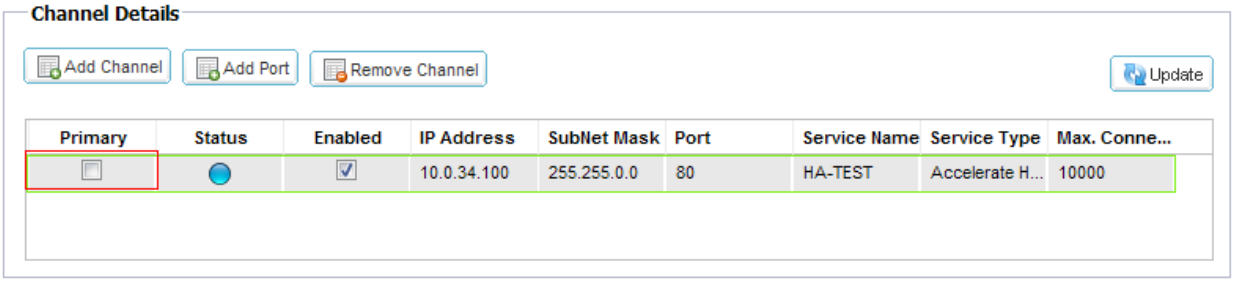


Failover Configuration

To setup load balancing on a channel click (Setup →IP Services). This will open the IP Service tab. 

.

A new tick box to enable this unit as the *Primary* box is now shown on each channel; click this box and then update:



This unit is now the primary ALB on this Channel.

Different jetNEXUS ALB's can be primary on different IP addresses.

See diagram above.

If the primary jetNEXUS ALB is unable to support any of the listening interfaces associated with the IP address, e.g. the primary is powered down or it loses contact with all content servers associated with the listening interface, a secondary jetNEXUS ALB will take over.

Configuring more than one content server for a listening interface causes jetNEXUS ALB to perform load balancing of requests across the content servers.

The policy used is *Least Connections.* This places each request on the content server with the least outstanding requests.

If jetNEXUS ALB is unable to contact a content server, jetNEXUS ALB removes the content server from the set, placing requests on the remainder.

If jetNEXUS ALB loses contact with all content servers, it removes support for that listening interface. In a fail over configuration, another jetNEXUS ALB will step into the breach.

Failover status lights

The coloured lights to the left of the listening interface shows the status:


Application server and or channel are providing service


Secondary channel is assessing primary service state


Listening interface is inactive, but in fail over standby ready to support it

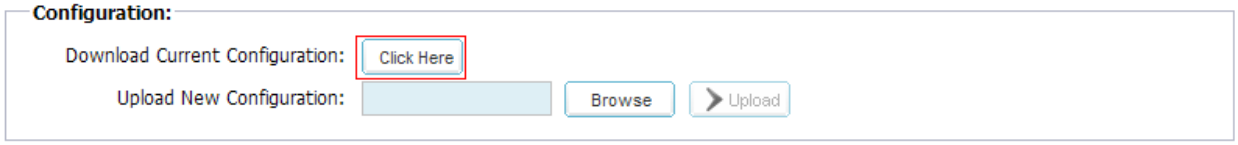
You have now configured a High Availability

ALB Maintenance

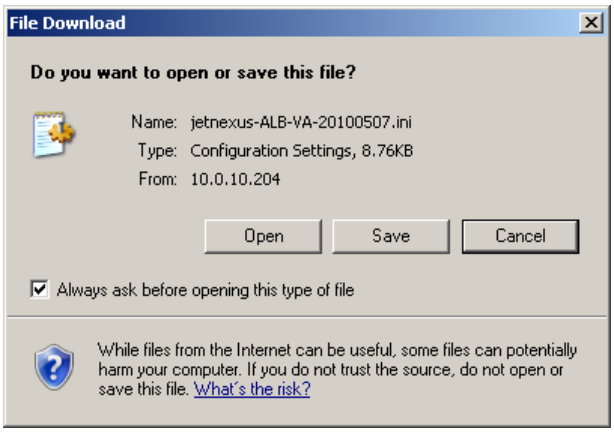
Backing up the ALB

Using the Navigation bar on the left of the web interface, go to (Advanced →Update Software). This will open the Update Software Tab

The current configuration can be downloaded and saved to your local machine using the Click Here button:



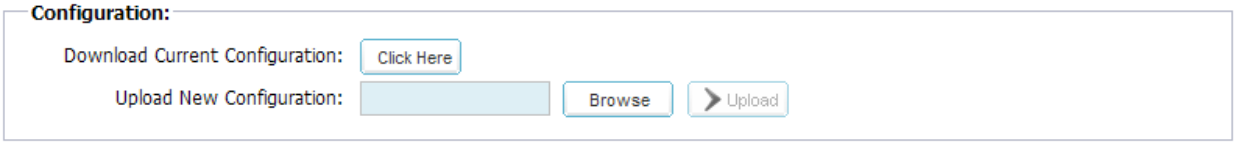
You will then be asked where to save the files:



Restoring the ALB

To restore a full configuration simply browse to the file under (Advanced →Update Software). This will open the update software Update Software tab.

To restore a full configuration simply browse to the file under "Upload new configuration" browse and find your configuration and click go:

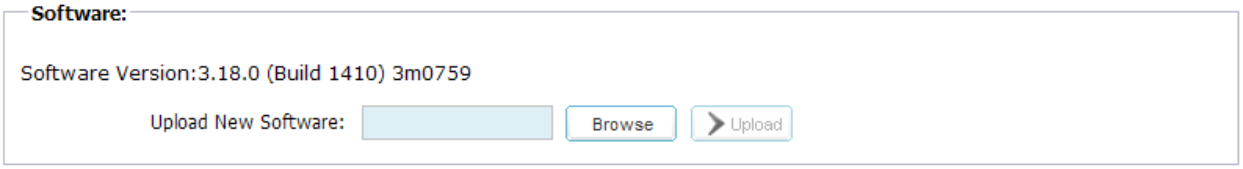


This will cause a brief software restart. There are also configuration updates that can be uploaded in the same way.

Updating the Software

All software upgrades for the ALB can be performed via the web interface. They are performed in the same way as uploading a new configuration file, using the second upload box called "Upload New Software."

The version of software currently running is shown for reference:

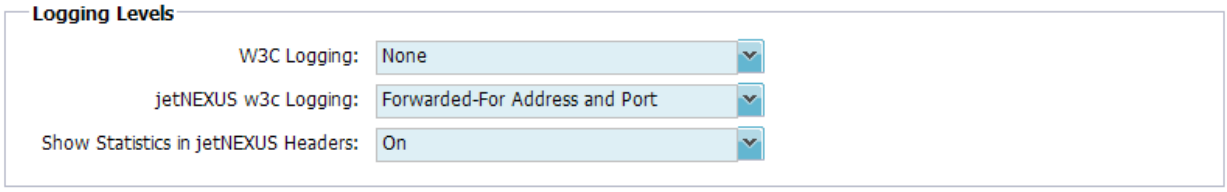


Configuring Logging

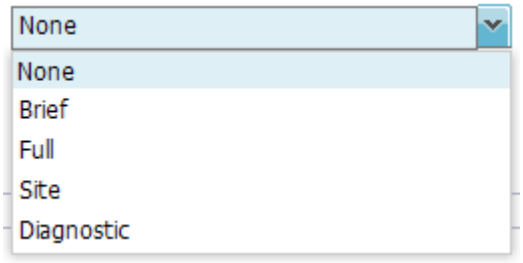
The ALB supports full W3C logging. This can be configured under (Configure →logging). This will open the 

tab.

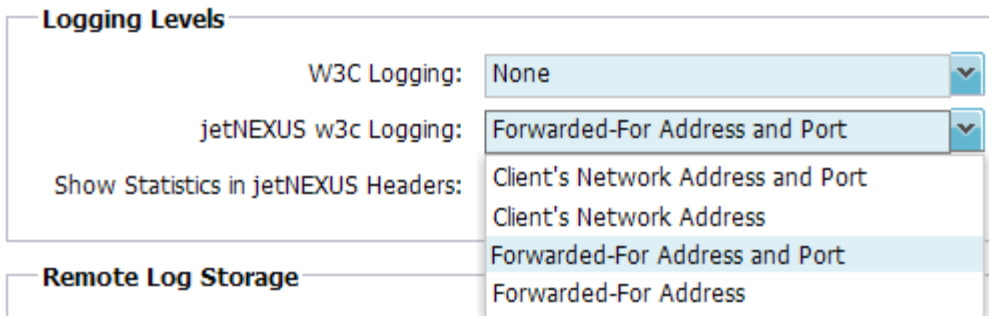
The W3C drop down allows you to set the Logging:



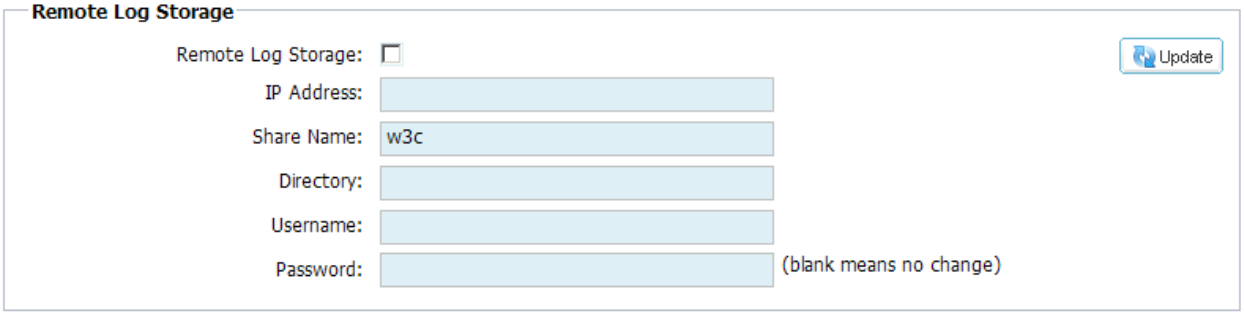
By default you should use "Full" or "Site." Use "Diagnostic" only if required to do so by a jetNEXUS engineer as it puts additional load on the device and consumes more file space:



The jetNEXUS w3C logging allows you to choose what you would like as the client source IP. If there is a proxy up stream of the device then you may wish to choose the X-Forwarded-For Address:

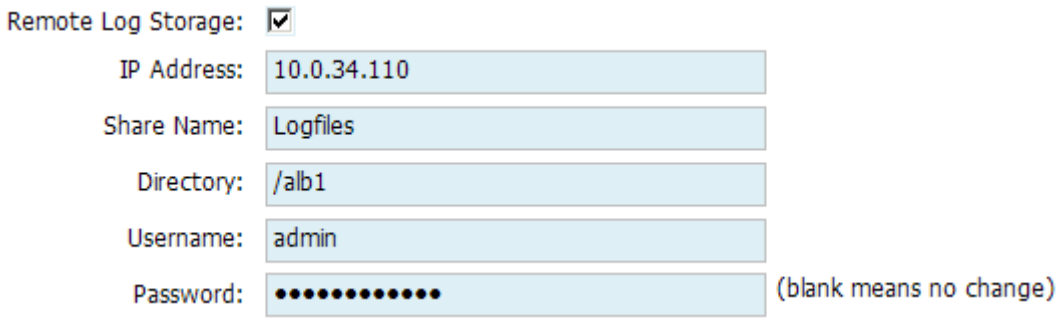


Remote storage is a facility whereby ALB copies w3c log files to a SMB/cifs network share:



Enter the details for the network share and tick the box to enable remote log storage. Each half hour, ALB checks for new log files and copies them to the network share.

Enter the details for the network share and tick the box to enable remote log storage. Each half hour, ALB checks for new log files and copies them to the network share:



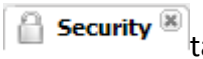
This must be a "local machine user account" o access the share[1] and cannot be a domain\username login.

Please observe restrictions on passwords for the remote log storage user. Avoid use of **£ $ / . * ? < > - &** and all types of quotes.

This account will need file create and file write access as well as read access to the directory.

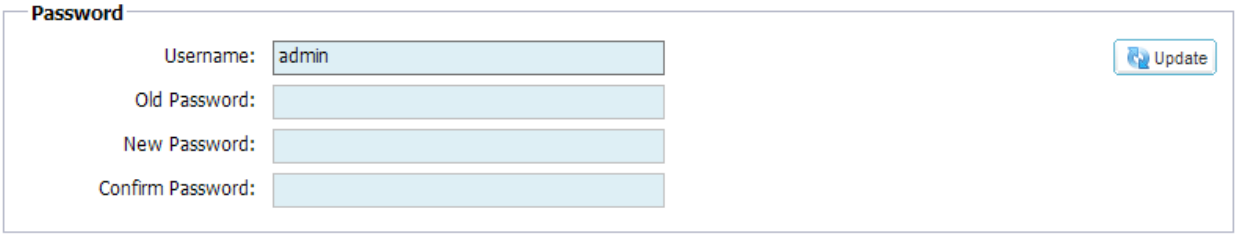
This is true for both the SMB/cifs share itself and the shared directory underneath on the host filing system.

Passwords and security

The passwords and access to the SSH shell can be configured under (Configure → Security). This will open the 

tab.

To change the password for the default Admin user, enter the old password and new password twice. Then click *Update* to apply the new configuration to the appliance:



Once you apply the new configuration, the new password is in effect. The browser therefore challenges you for an appropriate username and password to access the page:

Secure Shell Remote Connection is an option to allow SSH (SSH Transport Layer Protocol[2]) access to jetNEXUS Console.

[2] M. Friedl, N. Provos, and W. A. Simpson, Diffie-Hellman Group Exchange for the SSH Transport Layer Protocol, draft-ietf-secsh-dh-group-exchange-01.txt, April 2001, work in progress material.

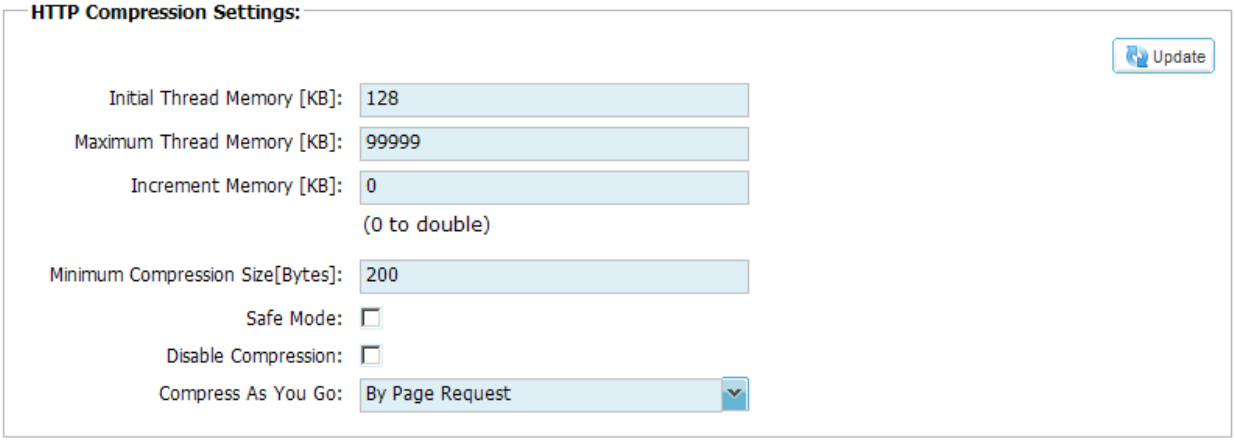
Acceleration and compression (advanced configuration)

Using the Navigation bar on the left of the web interface, go to (Advanced→*Protocol*→HTTP) this will open the Http Tab:

WARNING

Take extreme care when adjusting these settings as inappropriate settings can adversely affect the performance of ALB

The ALB- X has a powerful configurable compression engine:



Initial Thread Memory Allocation

The amount of memory each request received by jetNEXUS may initially allocate. For most efficient performance, this value should be set at a value just in excess of the largest uncompressed HTML file that the web servers are likely to send.

Maximum Thread Memory

The maximum amount of memory that jetNEXUS ALB will allocate on one request. For maximum performance, jetNEXUS normally stores and compresses all content in memory. If an exceptionally large content file exceeding this amount is processed, The ALB will write to disk and compress the data there.

Increment Memory

The amount of memory added to *Initial Thread Memory Allocation* when more is required. The default setting is zero. This means that the ALB will double the allocation when the data exceeds current allocation (e.g. 128 Kb, then 256 Kb, then 512 Kb, etc) up to the limit set by

Maximum Memory Usage per Thread. This is efficient where the majority of pages are of a consistent size but there are occasional larger files. (e.g. Majority of pages are 128Kb or less, but occasional responses are 1Mb in size). In the scenario where there are large variable sized files, it is more efficient to set a linear increment of a significant size (e.g. Responses are 2 Mb to10 Mb in size; an initial setting of 1Mb with increments of 1Mb would be more efficient).

Minimum Compression Size

The size, in bytes, under which jetNEXUS will not attempt to compress. This is useful because anything much under 200-bytes does not compress well and may even grow in size due to the overheads of compression headers.

Safe Mode

This option prevents the jetNEXUS-ALB from applying compression to style sheets or JavaScript. The reason for this is that even though the jetNEXUS ALB is aware of which individual browsers can handle compressed content, some other proxy servers, even though they claim to be HTTP/1.1 compliant are unable to transport compressed style sheets and JavaScript correctly. If problems are occurring with style sheets or JavaScript though a proxy server, then use this option to disable compression of these types. However, this will reduce the overall amount of compression of content.

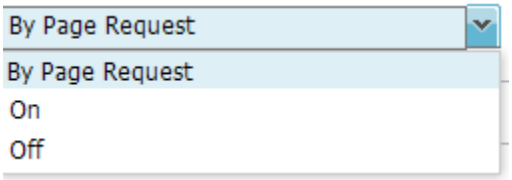
Disable Compression

Stops jetNEXUS from compressing any response.

Compress as you Go

Is an option to modify the buffering of the sever response.

There are three settings:



By Page request

Each page will need to have a header to let ALB know that you want to chunk the response.

On

Compress as you go will be enabled on all pages

Off

Compress as you go will not be used

Compression Exclusions

To exclude files from compression, go to (Advanced→*Protocol*→HTTP) This will open the HTTP Tab 

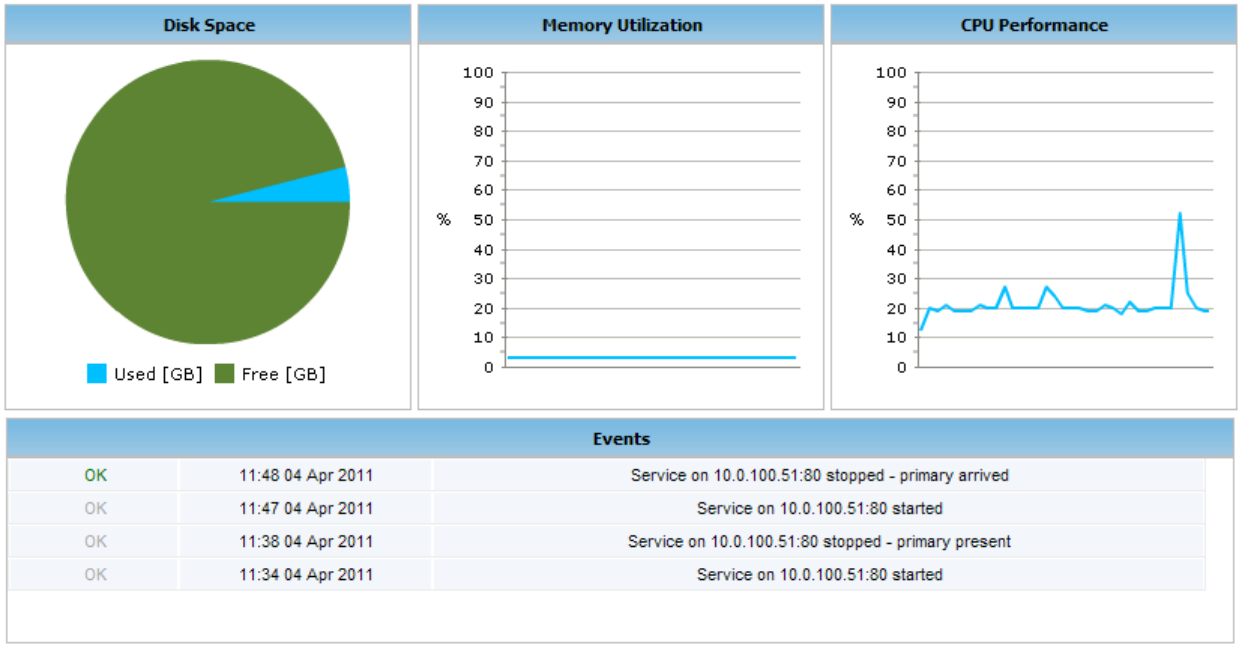
Add a line into the *Current Exclusions* fields for file or files that are not to be compressed:.

In the example above, all JavaScript files in the /exchweb/controls/ folder will be excluded from compression.

Monitoring

Using the Navigation bar on the left of the web interface, click on the Home button, this will open the Dashboard tab:

Dashboard



Disk Space

Gives an indication on how much disk space is being used by the jetNEXUS ALB.

Memory Indication Bar

Gives an indication on how much system memory the jetNEXUS ALB is using.

CPU Indication Bar

Gives an indication of the current CPU load on the jetNEXUS ALB.

Events

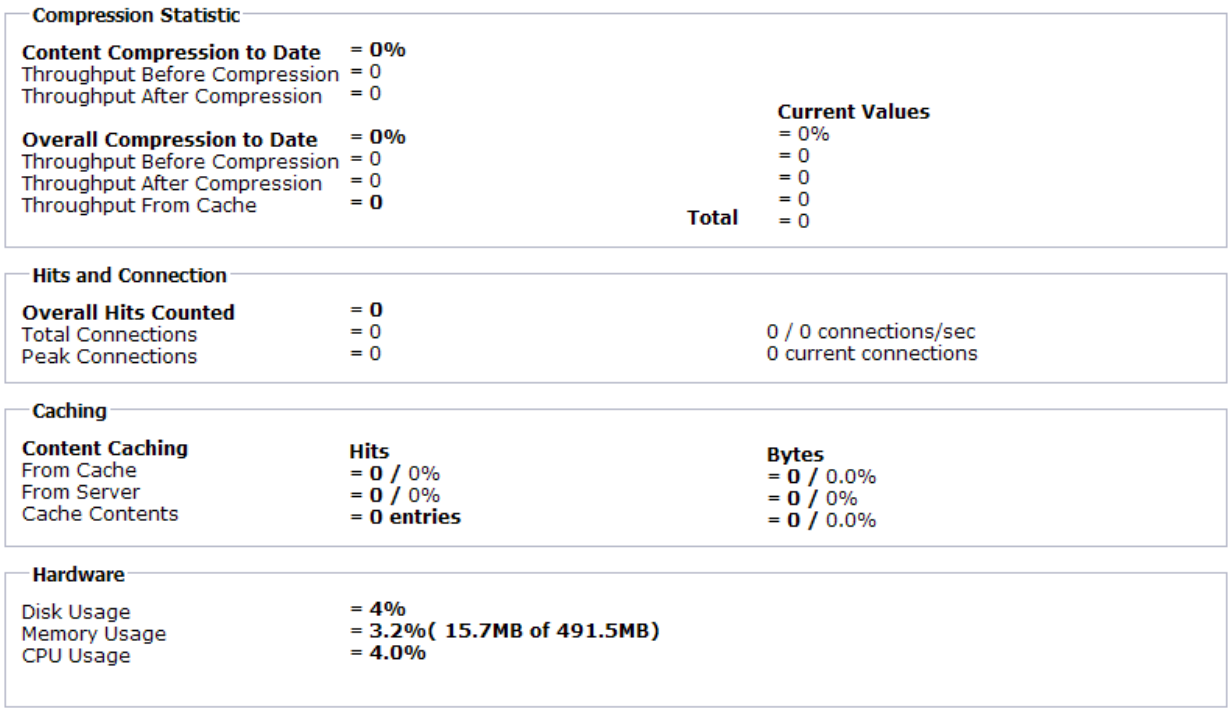
Under the graphics is a rolling log the highlight of the system log. Information such as content server coming on and off line and services starting and stopping are displayed:

Events		
OK	11:48 04 Apr 2011	Service on 10.0.100.51:80 stopped - primary arrived
OK	11:47 04 Apr 2011	Service on 10.0.100.51:80 started
OK	11:38 04 Apr 2011	Service on 10.0.100.51:80 stopped - primary present
OK	11:34 04 Apr 2011	Service on 10.0.100.51:80 started

Statistics

Using the Navigation bar on the left of the web interface, go to (Monitor →Statistics), this will open the Statistics tab:

Default statistics screen



Compression Statistic

Content Compression to Date	= **0%**	
Throughput Before Compression	= 0	
Throughput After Compression	= 0	
		Current Values
Overall Compression to Date	= **0%**	= 0%
Throughput Before Compression	= 0	= 0
Throughput After Compression	= 0	= 0
Throughput From Cache	= **0**	= 0
	Total	= 0

Hits and Connection

Overall Hits Counted	= **0**	
Total Connections	= 0	0 / 0 connections/sec
Peak Connections	= 0	0 current connections

Caching

Content Caching	**Hits**	**Bytes**
From Cache	= **0** / 0%	= **0** / 0.0%
From Server	= **0** / 0%	= **0** / 0%
Cache Contents	= **0 entries**	= **0** / 0.0%

Hardware

Disk Usage	= **4%**
Memory Usage	= **3.2%(15.7MB of 491.5MB)**
CPU Usage	= **4.0%**

The *Content Compression to Date* percentage is the amount by which jetNEXUS ALB has reduced compressible content (e.g. Text, HTML, Style sheets etc). A higher figure indicates better compression rates.

The *Throughput before compression* figure shows the number of bytes that WOULD have been transmitted if jetNEXUS had not compressed the data.

The *Throughput after Compression* figure show the ACTUAL number of bytes transmitted.

The *Overall Compression to Date* percentage is the amount by which jetNEXUS has reduced all output from the server including the overhead of those items that it did not compress.

Note: The jetNEXUS ALB counts compression statistics only for requests from browsers that accept compression.

If content caching is enabled (ALB-X) then additional statistics will be displayed related to caching performance.

From Cache

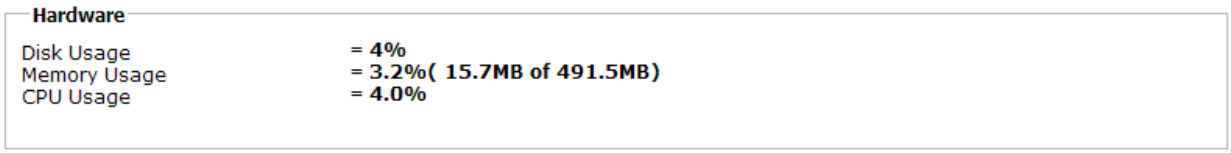
Number of byte and hits that are served from the jetNEXUS device.

From server

Number of Bytes or hits that are served from the content servers.

Cache Contents

Size and number of objects stored in the cache:



The *CPU usage*

Percentage indicates the loading on jetNEXUS Accelerator's CPU.

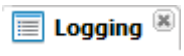
The *Memory usage*

Percentage indicates how much memory jetNEXUS ALB is currently using.

Overall Hits Counted

The number of requests received by jetNEXUS ALB whether or not content was compressed:

Logging

Using the Navigation bar on the left of the web interface, go to (Monitor →Logging), this will open the 

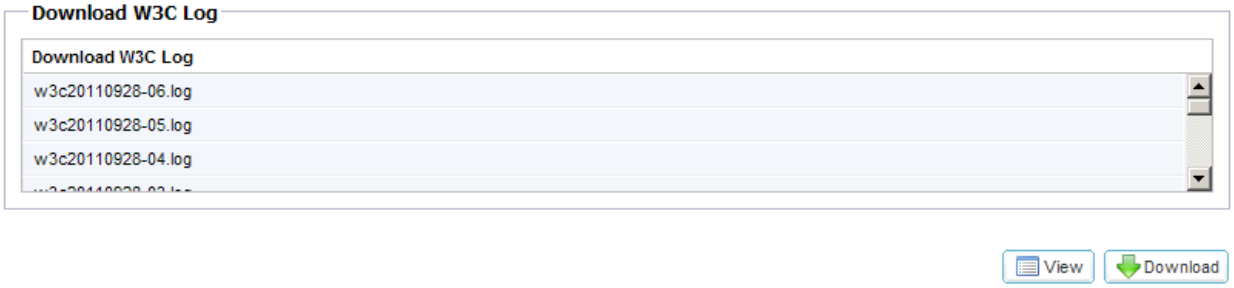
tab.

As discussed earlier in the manual *W3C Logging mode* will start jetNEXUS ALB recording a W3C compatible log file of activity.

Download W3C Log

This will download the W3C compatible log from ALB. The format of the file name is:

w3cyyyymmdd.log where (yyyy = year 2000 onwards, mm = month 1-12, dd = day 1-31)

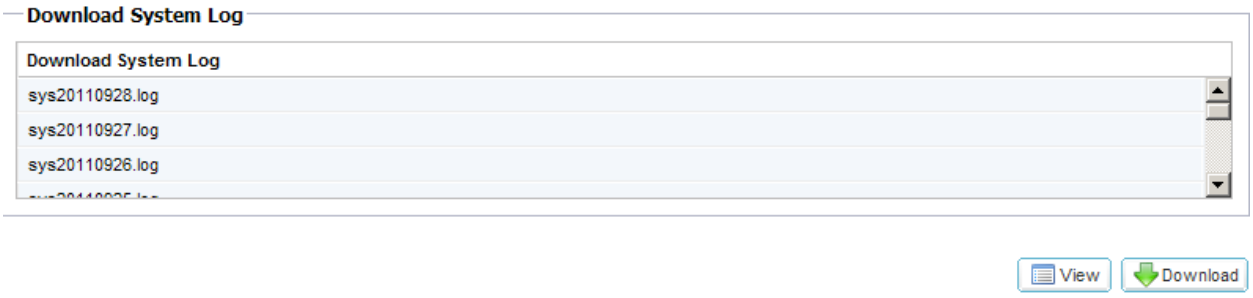


jetNEXUS WC£ logs are compatible with the w3c draft standard for web server logs and should be compatible with most analysis tools.

Download System Log

This will download the event log for the appliance. The format of the file name is:

sysyyyymmdd.log where (yyyy = year 2000 onwards, mm = month 1-12, dd = day 1-31)



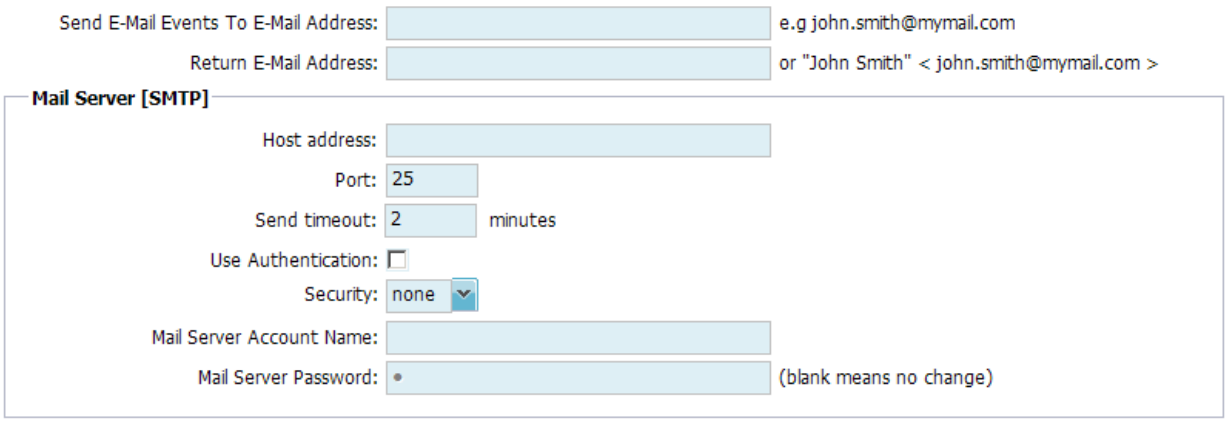
Email Events

Using the Navigation bar on the left of the web interface, go to (Configure → Email Events) this will open the E-Mail Events tab

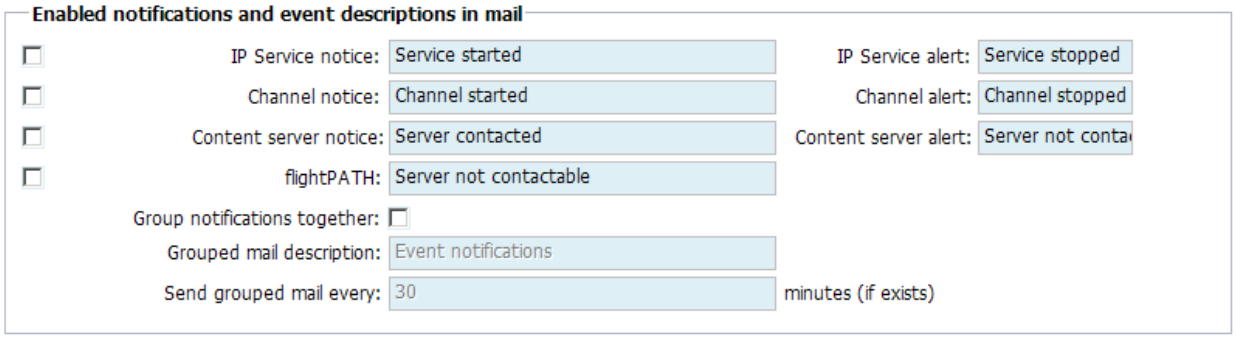
What can you set?

The ALB can be configure to automatically send email alerts on key events such as losing service, Overheating, device rebooting, interfaces being raised or lowered, contents servers coming on and off line etc.

Mail Server [SMTP] Setup:



Send E-Mail Events To E-Mail:	**e.g. support@jetNEXUS.com**
Return E-Mail Address:	**e.g. support@jetNEXUS.com**
Host address:	**IP or FQDN**
Port:	**25**
Send Timeout:	**2**
Use Authentication:	**If required by your mail server**
Security:	**If required by your mail server**
Mail Server Account Name:	**username**
Mail Server Password:	**password**



All Values below can be modified you meet your specific message requirements:

IP Service notice: **Service Alert Message title**

IP Service alert: **Service Stopped Alert**

Channel notice: **Channel Alert Message title**

Channel alert: **Channel Stopped Alert**

Content server notice: **Content Message title**

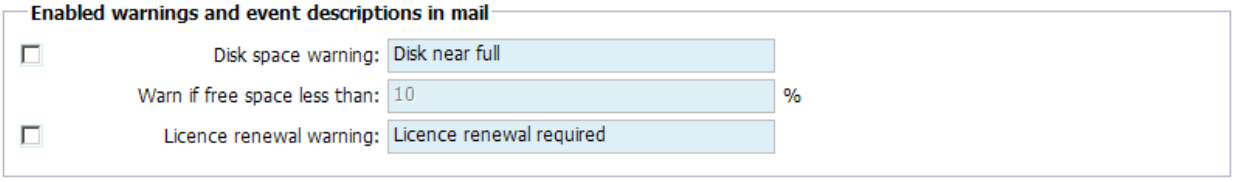
Content server alert: **Channel Alert**

flightPATH: **FlightPATH Message title**

Group notifications together: **All alerts into a single e-mail alert**

Grouped mail description: **Grouped Message title**

Send grouped mail every: **Time for alerts to be sent**



Disk Space warning: **Disk near full message**

Warn if free space less than: **Percentage of disk before alert**

License renewal warning: **License renewal required**

Services

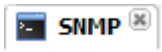
The *Services* menu provides pages to allow the following actions to carried out on the jetNEXUS ALB (Services).

The menu provides the followings tabs:

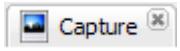
Date and Time

Ping

SNMP



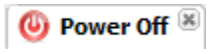
Capture



Restart

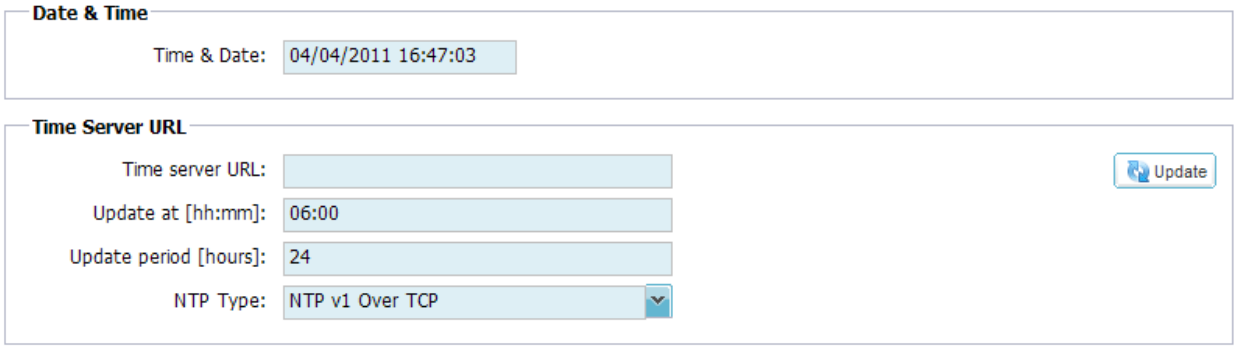
Reboot

Power Off



Date and Time

Simply enter the new time (UTC format and Click on update):



The Appliance also supports NTP the Appliance also supports NTP.

Time Server URL

Timeserver URL allows jetNEXUS ALB to connect to an SNTP time server. If jetNEXUS ALB has a gateway that also provides a DNS facility, a URL works too. In most circumstances, it is better to resolve the DNS name into an IP Address and use it instead.

Update time:

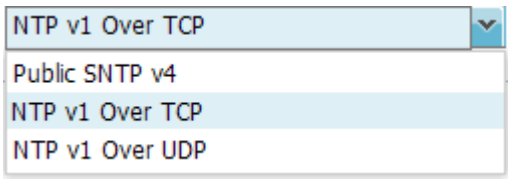
Update at is the time of day that jetNEXUS ALB contacts the SNTP time server. This controls what times of day the time corrections will happen.

Update period:

Update period states how often jetNEXUS ALB should consult the SNTP time server. This might be 24, 6 or 1 as required. Fractional hours are valid too if needed.

NTP method:

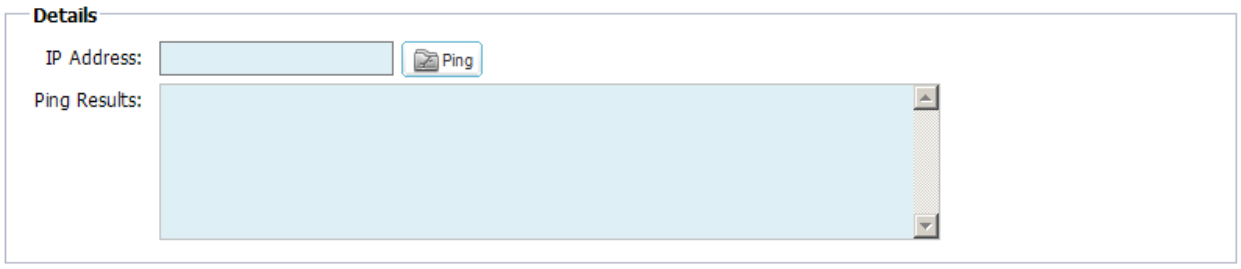
The SNTP time server protocol standard is selected using the drop-down box. Supported settings are:



You will see time corrections carried out in the System Log. JetNEXUS ALB logs both successful and unsuccessful attempts. Successful updates also show any time discrepancy.

Ping

The ping tool can be used to check network connectivity:

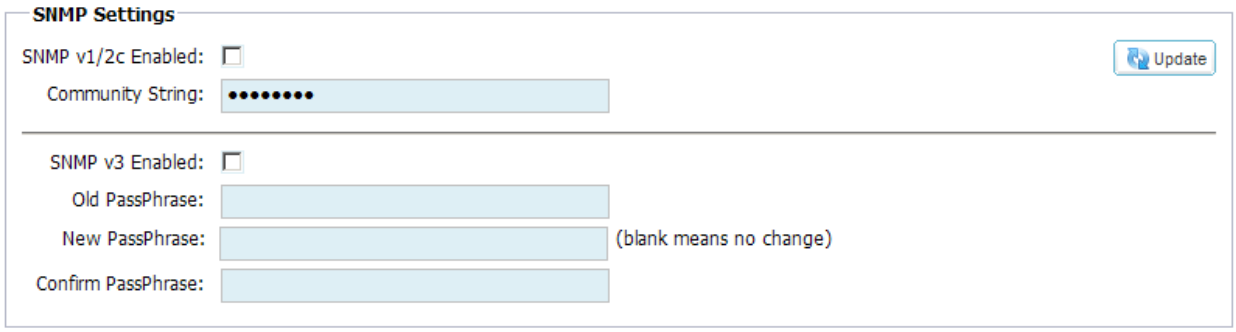


IP Address is where to enter the IP Address of the device to contact with an echo test.

Click *Ping* to perform the echo test. Four attempts are made to contact the device. The text area displays the results on completion.

SNMP

Setting up the jetNEXUS ALB to provide a Simple Network Management Protocol:



SNMP v1/2c *Enabled* allows SNMP version 1 and version 2c access using the specified *Community String*. The default community string is jetNEXUS.

SNMPV3 *Enabled* allows SNMP V3 for a single user admin with the default *Passphrase* jetNEXUS. To change the Passphrase, enter the old Passphrase, the new Passphrase twice and click *Update*.

**JetNEXUS ALB SNMP security settings are separate from other security settings on ALB. Set them independently to values required by the management infrastructure.

Capture

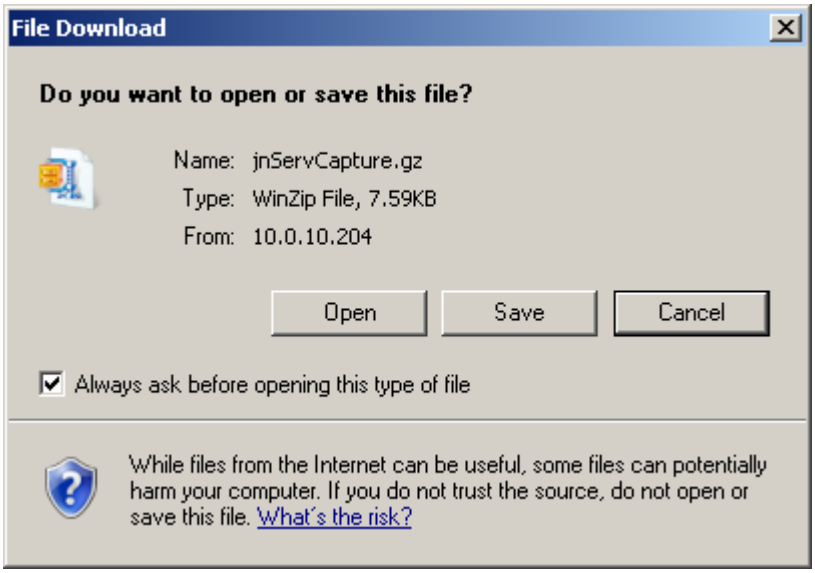
Capture is a useful debugging tool, you may be asked to use this by the jetNEXUS support team when trying to troubleshoot an issue:

Adapter: The adapter from where you want the trace

Packets: The number of packets you want collected

Duration: The duration in seconds of the trace

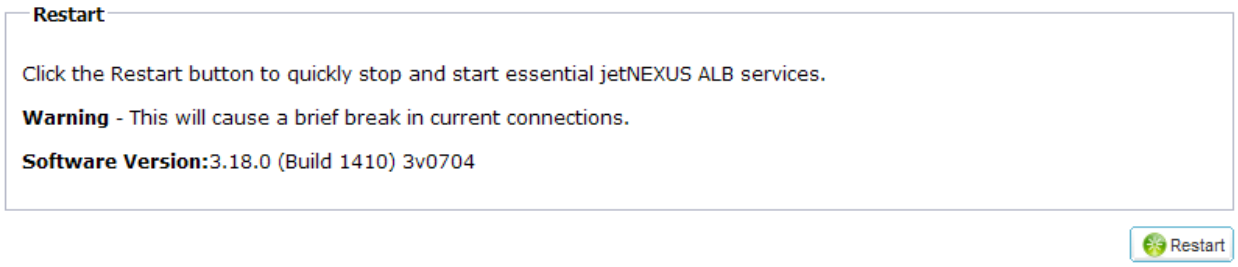
Click the Generate button:



The file will be returned to the browser in a GZ form.

Restart

To initiate the restart operation click *Restart*:

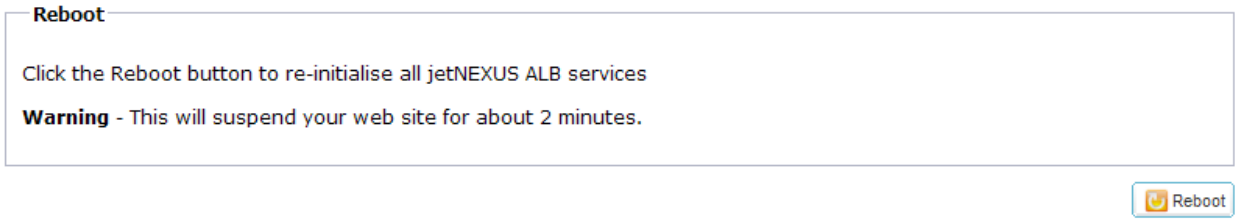


Note: It can take up to 30 seconds for jetNEXUS ALB to restart.

Reboot

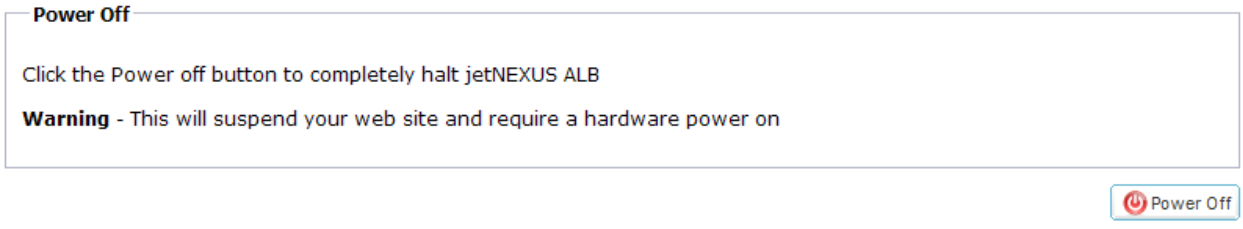
To initiate a reboot, click *Reboot*.

Note: It can take a couple of minutes for the jetNEXUS to reboot:



Power Off

To initiate power-off, click *Power Off*:



Note: To restart jetNEXUS, a hardware power on will be required.

Note:
In the event of power supply loss, jetNEXUS ALB will automatically power on again when power is reconnected.

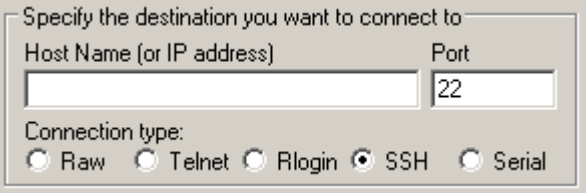
CLI (Command line interface)

The command line interface is designed to only configure that basic settings of the so that the device and bring up and its web interface for further configuration. In addition to this the CLI can be used to reset the device to its factory defaults.

Accessing the CLI

The CLI can be accessed by three methods:

SSH client (assuming it has not been disabled in the configuration)



Serial (RS232) connection (9600 parity 8 Bits)

Connect to the device using one of the methods as described above

Log into the console with the following credentials:

Username: admin
Password: jetnexus

```
login as: admin
admin@10.0.10.204's password:
Last login: Thu May  6 13:39:32 2010
--> -jetnexusconfig <--
Welcome to the jetNEXUS configurator v3.0.3 (Build 158)
Type 'quit' to exit.

Command:
```

To change the management IP address run the following command:

Command: set greenside=x.x.x.x

You will then be told the **Greenside** has been changed

To change the subnet mask:

Command: Set mask eth0 X.X.X.X

You will then be told the **Greenside** has been changed

You can check your changes by running the show command for example (show **greenside** IP).

If you need to change the default gateway you need to run the following command. In this example it will change it to 192.168.10.1. Be careful when changing the gateway remotely as if you get it wrong you may have a long drive!

Command: route add default gw 192.168.10.1

To return the device to the factory defaults type the following:

Command: defaults

To exit this CLI type *exit*

jetNEXUS Help

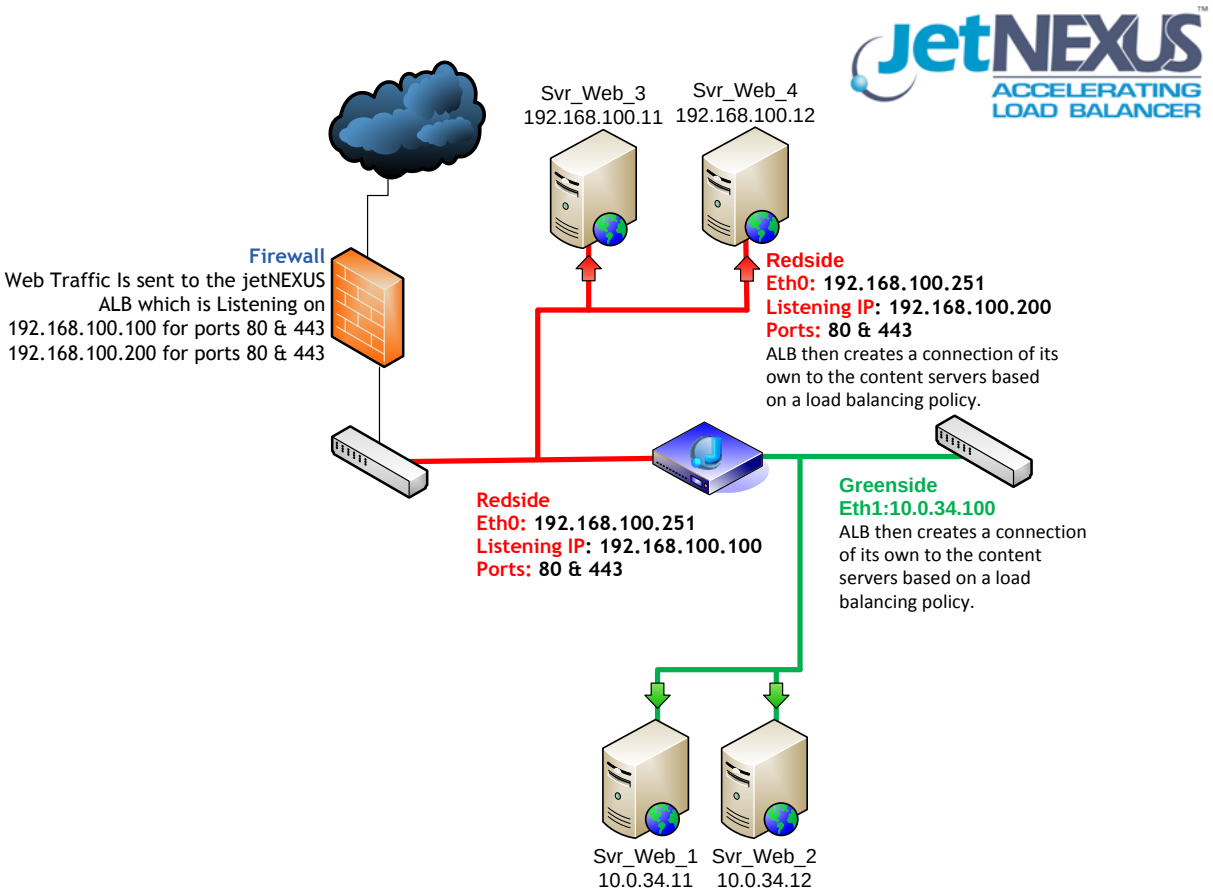
FAQ's

Q: How much improvement will I achieve compared to uncompressed web sites?

A: That will very much depend on the design of the website and in particular the graphic content. Typically our customers see a 40%-60% reduction in bandwidth usage and a 30%-50% improvement in total page download times.

Q: Can the ALB also support content servers on any interface.

A: Yes, the ALB can support content servers on any interface depending on your use of channel configurations. Please contact support@jetNEXUS.com if you wish to enable this configuration and you are having issues.



Troubleshooting

Further help can be found on the jetNEXUS websites

http://www.jetNEXUS.com/support.html

http://forum.jetNEXUS.com/

Contact US

I hope you have found this User Manual informative, but if you need any clarification or further information, please do not hesitate to get in contact with jetNEXUS Support:

E-mail support@jetNEXUS.com

Support +44 (0870) 382 5529

Phone+44 (0870) 382 5550

Check out our blog
 HYPERLINK "http://jetnexus.blogspot.com/" *http://jetNEXUS.blogspot.com/*